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

Erman İŞIK, Yasemin KARA, Ekin OZMAN
Department of Mathematics, Faculty of Arts and Sciences, Boğaziçi University, Istanbul, 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 $O_K$ 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 $x, y, z \in O_K$ 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 $a, b, c \in O_K$ 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.
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
\[
a^p + b^p = c^2, \quad a, b, c \in \mathcal{O}_K
\] (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 \( \cup_{p \text{ prime}} C_p(K) \) 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, \( \cup_{p \text{ prime}} C_p(K) \) 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 \((ac, bc, c^{p+1})\) 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 \( K(S_K, n) = \{ x \in K^*/K^{*n} : v_p(x) \equiv 0 \mod n, \forall \mathfrak{p} \notin S_K \} \). It is known that \( K(S_K, n) \) is a finite abelian group ([20], sections 5.2.2 and 7.4). Now, let \( L = K(\sqrt{\alpha}) \) for \( a \in K(S_K, 2) \) and define \( S_L = \{ \mathfrak{P}' : \mathfrak{P}' \text{ is prime of } \mathcal{O}_L \text{ such that } \mathfrak{P}'|2 \} \text{ and } T_L = \{ \mathfrak{P}' \in S_L : \mathfrak{P}'|\mathfrak{P} \text{ for some } \mathfrak{P} \in T_K \} \).

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 \( L = K(\sqrt{\alpha}) \). Suppose that for every solution \((\lambda, \mu)\) to the \( S_K \)-unit equation
\[
\lambda + \mu = 1, \quad \lambda, \mu \in \mathcal{O}_K^*, \tag{1.2}
\]
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 \((\lambda, \mu)\) to the \( S_L \)-unit equation \( \lambda + \mu = 1, \quad \lambda, \mu \in \mathcal{O}_L^* \), 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, \( \cup_{p \text{ prime}} (C(K) \cap W_K) \) 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 \( f \) 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 \( f \) 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 \( (\lambda, \mu) \) 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 \( v_{\mathfrak{P}}(\lambda), v_{\mathfrak{P}}(\mu) \), 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 \( \sigma(p, q, r) = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} \), 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 \( x^2 + y^3p = z^5 \) 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 \( \eta_{E, p} \) denote the mod \( p \) Galois representation of \( E \). We use \( q \) for an arbitrary prime of \( K \), and \( G_q \) and \( I_q \) respectively for the decomposition and inertia subgroups of \( G_K \) at \( q \). 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.

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

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

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

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

\[ E = E_{a,b,c} : Y^2 = X^3 + 4cX^2 + 4a^pX. \] (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 $K$, 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 $q|p$, then $\rho_{E,p}$ 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 $N_E$. Let $p$ be a rational prime. Define the following quantities

$$M_p := \prod_{q \mid N_E, \ p \mid \nu_q(\Delta_q)} q, \text{ and } N_p := \frac{N_E}{M_p},$$

where $\Delta_q$ is the minimal discriminant of a local minimal model for $E$ at $q$. For a Hilbert eigenform $f$ over $K$, we write $Q_f$ for the field generated by its eigenvalues.

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

1. $p \geq 5$, the ramification index $e(q/p) < p - 1$ for all $q|p$, and $Q(\zeta_p)^+ \not\subseteq K$,
2. $E$ is modular,
3. $\rho_{E,p}$ is irreducible,
4. $E$ is semistable at all $q|p$,
5. $p|\nu_q(\Delta_q)$ for all $q|p$.

Then there is a Hilbert eigenform $f$ of parallel weight 2 that is new at level $N_p$ and some prime $\varpi$ of $Q_f$ such that $\varpi|p$ and $\rho_{E,p} \sim \rho_f$.
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 $f$ be a Hilbert newform of level $N$ and parallel weight 2 and with rational eigenvalues. Then there is an elliptic curve $E_f/K$ with conductor $N$ having the same $L$-function as $f$.

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 $f$ be a Hilbert newform over $K$ of level $N$ and parallel weight 2, such that $Q_f = Q$. Suppose either:

(i) $[K : Q]$ is odd; or

(ii) there is a finite prime $q$ such that $v_q(N) = 1$.

Then there is an elliptic curve $E_f/K$ of conductor $N$ with the same $L$-function as $f$.

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 $\rho_{E,p}$ is irreducible, and $\rho_{E,p} \sim \rho_{f,p}$ for some Hilbert newform $f$ over $K$ of level $N$ and parallel weight 2 which satisfies $Q_f = Q$. Let $q \nmid p$ be a prime ideal of $O_K$ such that:

(a) $E$ has potentially multiplicative reduction at $q$,

(b) $p \nmid \#\rho_{E,p}(I_q)$,

(c) $p \nmid (\text{Norm}_{K/Q}(q) \pm 1)$

Then there is an elliptic curve $E_f/K$ of conductor $N$ having the same $L$-function as $f$.

3. Frey curve and related facts

3.1. Behaviour at odd primes

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

$$E : Y^2 = X^3 + 4wX^2 + 4uX$$

whose arithmetic invariants are given by $\Delta_E = 2^{12}u^2v$, $j_E = 2^{6}(u + 4v)^3$, 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 $q \nmid 2$ be a prime ideal of $O_K$ and

$$s = \min\{v_q(u), v_q(v), v_q(w)\}.$$ 

Write $E_{\text{min}}$ for a local minimal model at $q$. Then we have the following:
3.2. Conductor of the Frey curve

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

\[ v_q(u) = v_q(v) = 2v_q(w). \tag{3.2} \]

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

\[ v_q(\Delta_q) = 2v_q(u) + v_q(v) - 6s. \]

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

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

Now we may use the change of coordinates

\[
\begin{align*}
X &\mapsto t^2X', \\
Y &\mapsto t^3Y',
\end{align*}
\]

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

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 \( \mathcal{O}_K/\mathfrak{P} \simeq F_2 \). 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 \( \Delta_E = 2^{12}(a^2b)^p, \ j_E = 2^9(4b^p + a^p)^3 \)
\((a^2b)^p), \) and the conductor \( \mathcal{N}_E \). Recall also the quantities

\[ \mathcal{M}_p = \prod_{q \mid \mathcal{N}_E, \ p \nmid v_q(\Delta_q)} q, \text{ and } \mathcal{N}_p = \mathcal{N}_E/\mathcal{M}_p, \]

where \( \Delta_q \) is the minimal discriminant of a local minimal model for \( E \) at \( q \).
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 \(N_E\). Then, for all primes \(q \notin S_K\), the model \(E\) is minimal, semistable and satisfies \(p|v_q(\Delta_E)\). Moreover,

\[
N_E = \prod_{\mathfrak{p} \in S_K} \mathfrak{p}^{r_p} \prod_{q|ab, \ q \text{ odd prime}} q, \quad N_p = \prod_{\mathfrak{p} \in S_K} \mathfrak{p}^{r^p},
\]

where \(0 \leq r_p^q \leq r_p \leq 2 + 6v_p(2)\).

Proof Let \(q\) 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 \(q\) divides \(\Delta_E\), so \(q|ab\). Since \(a\) and \(b\) are relatively prime, \(q\) divides exactly one of \(a\) and \(b\). Therefore, \(q\) does not divide \(c_4\). By Lemma 3.1, \(E\) has multiplicative reduction at \(q\) and is minimal. Hence, \(p|v_q(\Delta_E) = v_q(\Delta_q)\). By the definition of \(N_p\), \(q' N_p\). By \([49, \text{Theorem IV.10.4}]\), \(r = v_q(N_E) \leq 2 + 6v_p(2)\).

\(\square\)

3.3. Images of Inertia

Now, we collect some necessary information about images of inertia \(\overline{\rho}_{E,p}(I_q)\). 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 \(p \geq 5\) and \(q \nmid p\) be a prime of \(K\). Then \(p|\#\overline{\rho}_{E,p}(I_q)\) if and only if \(E\) has potentially multiplicative reduction at \(q\) (i.e. \(v_q(j_E) < 0\)) and \(p \nmid v_q(j_E)\).

By using the previous result we obtain:

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

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

\(\square\)

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

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

\(\square\)

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 \((a, b, c)\) be \(W_K\) 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:

\[\text{1204}\]
(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 $\mathfrak{P} \in T_K$, $\nu_{\mathfrak{P}}(j_{E'}) < 0$ 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 $\overline{\rho}_{E,p} \sim \overline{\rho}_{f,\mathfrak{P}}$ for some Hilbert newform $f$ of level $\mathcal{N}_p$ and some prime $\mathfrak{P}$ of $\mathbb{Q}_f$ where $\mathbb{Q}_f$ denotes the field generated by the Hecke eigenvalues of $f$.

Now we reduce to the case where $\mathbb{Q}_f = \mathbb{Q}$, 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 $f$. 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 $p \nmid (\text{Norm}_{K/\mathbb{Q}}(\mathfrak{P}) \pm 1)$.

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 $\#(\text{Tors}E''(K)) \equiv 0 \pmod{2}$. 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 $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$.

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 $\nu_{\mathfrak{P}}(j_{E'}) < 0$. \hfill $\square$

**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 $p$ of $K$ at which $E$ has good reduction let $N(p)$ denote the number of $\mathbb{F}_p$-rational points on $E$ mod $p$. If we have

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

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

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

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 $\lambda$-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 $\bar{K}$) 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

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

Let $S_3$ denote the symmetric group on three letters. The action of $S_3$ on the set $\{e_1, e_2, e_3\}$ can be extended 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 $S_3$, the orbit of $\lambda$ in $\mathbb{P}^1(K) - \{0, 1, \infty\}$, called $\lambda$-invariants, is the set:

$$\left\{ \lambda, \frac{1}{\lambda}, \frac{1}{1 - \lambda}, \frac{1}{\lambda - 1}, \frac{\lambda - 1}{\lambda} \right\}. \quad (5.2)$$

Moreover, there is a one-to-one correspondence between the $\bar{K}$-isomorphism classes of the Legendre elliptic curves and the $S_3$-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 $\nu_p(j_{E'}) < 0$. 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-division 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 $\lambda$ be any of the $\lambda$-invariants of $E'$. As $E'$ has good reduction away from $S_K$, the $j$-invariant $j_{E'}$ belongs to $O_{S_K}$. From the equation (5.1), we can deduce that $\lambda \in K$ satisfies a monic polynomial with coefficients in $O_{S_K}$ implying $\lambda \in O_{S_K}$. On the other hand, notice that $1/\lambda, \mu := 1 - \lambda$ and $1/\mu$ are solutions of (5.1) and hence elements of $O_{S_K}$. Therefore, we conclude that $(\lambda, \mu)$ is a solution of the $S_K$-unit equation (1.2).

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

$$j_{E'} = 2^8 \frac{(1 - \lambda \mu)^3}{(\lambda \mu)^2}. \quad (5.3)$$
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 \( \lambda \) is the \( \lambda \)-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, \( L = K(\sqrt{\alpha}) \) 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 \( (a, b, c) \in \mathbb{W}_K \) 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 \( p \nmid v_\mathfrak{p}(j_{E'}) \). \( \Box \)

By applying Lemma 5.1 and Lemma 3.3 we see that \( p | \#\mathfrak{p}_{E,p}(I_{E'}) \), so \( p | \#\mathfrak{p}_{E',p}(I_{E'}) \). 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 \( \lambda \) be any of the \( \lambda \)-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 \( \lambda, \mu \) is a solution of the \( S_L \)-unit equation (1.2).

Now, by the assumption of the Main Theorem, for every solution \( (\lambda, \mu) \) 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 remaining 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 available 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


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


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

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


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

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