Asymptotic Fermat for signatures $(p, p, 2)$ and $(p, p, 3)$ over totally real fields

Diana Mocanu

Abstract

Let K be a totally real number field and consider a Fermat-type equation $a^l + b^m = c^n$ over K. We call the triple of exponents (l, m, n) the *signature* of the equation.
In this project we start with Işik, Kara and Ozman's work in [21] which gives a computable criteria of testing if the *asymptotic Fermat Last Theorem* holds for certain type of solutions of the equations with signatures $(p, p, 2)$. We first generalize this result by relaxing the assumption on the class number. Then, we use the same method involving modularity, lever lowering and image of inertia comparison to study the $(p, p, 3)$ equation. This approach was first developed by Freitas and Siksek in [29] and relies on a partial result towards the modularity conjecture for elliptic curves over totally real fields proved in [12].

Contents

1 Introduction

1.1 Historical background

The study of Diophantine equations is of great interest in Mathematics and goes back to antiquity. The most famous example of a Diophantine equation appears in *Fermat's Last Theorem.* This is the statement, asserted by Fermat in 1637 without proof, that the Diophantine equation $a^n + b^n = c^n$ has no solutions in whole numbers when n is at least 3, other than the trivial solutions which arise when $abc = 0$. Andrew Wiles famously proved the Fermat's Last Theorem in 1995 in his paper "Modular elliptic curves and Fermat's Last Theorem" [38]. The proof is by contradiction employing techniques from algebraic geometry and number theory to prove a special case of the modularity theorem for elliptic curves, which together with Ribet's lever lowereing theorem gives the long-waited result. Since then, number theorists extensively studied Diophantine equations using Wiles' modularity approach. Siksek gives a comprehensive survey about this method over the field of rationals in [29].
Even before Wiles announced his proof, various generalizations of Fermat's Last Theorem had already been considered, which is of the shape

$$Aa^p + Bb^q = Cc^r \tag{1}$$

for fixed integers A, B and C. We call (p, q, r) *the signature* of the equation (1). A *primitive* solution (a, b, c) is a solution where a, b and c are pairwise coprime and a *non-trivial* solution (a, b, c) is a solution where $abc \neq 0$.

In [21], Işik, Kara and Ozman list all known cases where equation (1) has been solved in integers in two tables (pg. 4). Table 1 contains all unconditional results for infinitely many primes. In Table 2, they give all conditional results.
We highlight here one relevant family of solutions, namely (p, p, k) where p is a rational prime and $k \in \{2, 3\}$. Darmon and Merel [8] and Poonen [23] proved the following theorem:

Theorem 1.1. *(i) The equation $a^n + b^n = c^2$ has no non-trivial primitive integer solutions for $n \geq 4$.*

(ii) The equation $a^n + b^n = c^3$ has no non-trivial primitive integer solutions for $n \geq 3$.

Note that the above equations, typically have infinitely many non-primitive solutions. For example, if n is odd, and a and b are any two integers with $a^n + b^n = c$, then

$$(ac)^n + (bc)^n = (c^{\frac{n+1}{2}})^2$$

giving a rather uninteresting supply of solutions. Thus, we would only study the primitive solutions of the above equations.
A naive sketch of the proof of Theorem 1.1 is as follows. First note that it is enough to prove the assumption for $n = p$ an odd prime. Suppose $a, b, c \in \mathbb{Z}$ is a non-trivial, primitive solution to (i) or (ii). In each of the cases, we can associate a so-called Frey elliptic curve $E_{a,b,c}/\mathbb{Q}$ and let $\overline{\rho}_{E,p}$ be its mod p Galois representation, where $E = E_{a,b,c}$. Then $\overline{\rho}_{E,p}$ is irreducible by Mazur [22] and modular by Wiles and Taylor [38] and [33]. Applying Ribet's lever lowering theorem [25] shows that $\overline{\rho}_{E,p}$ arises from a weight 2 newform of level 32 for (i) and level 27 for (ii). These are closely related to the modular curves $X_0(32)$ and $X_0(27)$ which turn out to be elliptic curves with complex multiplication. Darmon and Merel prove in [8], by using the theory of complex multiplication that this implies $j_E \in \mathbb{Z}[\frac{1}{p}]$ for $p > 7$, which gives a contradiction. The cases when $p \leq 7$ are treated in a more elementary way by Poonen [23].
Recently, important progress has been done towards generalisation of the modularity approach over larger fields. In [14] 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 i.e. the ones satisfying $abc = 0$. Then, Deconinck [9] extended the results of Freitas and Siksek [14] 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 [28] 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 [18] to the case of

generalized Fermat equation. Also, recently in [34] and [35] Ţurcaş studied Fermat equation over imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ with class number one.
Finally, we present a result by Işik, Kara and Ozman, proved in [21] which serves as the starting point of this project.
It gives a computable criteria of testing if the *asymptotic Fermat Last Theorem* holds for certain type of solutions of the equations with signatures $(p, p, 2)$.
To state it, we need the following notation:

$$S_K := \{\mathfrak{P} : \mathfrak{P} \text{ is a prime of } K \text{ above } 2\}, \quad T_K := \{\mathfrak{P} \in S_K : f(\mathfrak{P}/2) = 1\}$$
$$W_K := \{(a, b, c) \in \mathcal{O}_K^3 : a^p + b^p = c^2 \text{ with } \mathfrak{P}|b \text{ for every } \mathfrak{P} \in T_K\}$$

Note 1.2. When (a, b, c) are primitive (pairwise coprime), $\mathfrak{P}|b$ implies $\mathfrak{P} \nmid a$ and $\mathfrak{P} \nmid c$.

Theorem 1.3. *Let K be a totally real number field with narrow class number $h_K^+ = 1$. For each $a \in K(S_K, 2)$, let $L = K(\sqrt{a})$.*
(A):Suppose that for every solution (λ, μ) to the S_K-unit equation:

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

there is some $\mathfrak{P} \in T_K$ that satisfies $max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\} \leq 4v_{\mathfrak{P}}(2)$.
(B):Suppose also that for each L, for every solution (λ, μ) of the S_L-unit equation $\lambda + \mu = 1$, $\lambda, \mu \in \mathcal{O}_{S_L}^*$, 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 B_K - depending only on K- such that for each $p > B_K$, the equation $a^p + b^p = c^2$ has no primitive, non-trivial solutions with $(a, b, c) \in W_K$ (i.e. the asymptotic Fermat holds for W_K).

Remark 1.4. Inspired by this result:

- we would like to find a more general assumption on the class group $\mathrm{Cl}(K)$ of K for which this result holds. It turns out that requiring $\mathrm{Cl}_{S_K}(K)[2]$ to be trivial is enough.
- we will rephrase the theorem without imposing separate constraints on the extensions L/K.

However, these will come at an expense of solving an equation of the form:

$$\alpha + \beta = \gamma^2,\ \alpha, \beta \in \mathcal{O}_{S_K}^*,\ \gamma \in \mathcal{O}_{S_K}$$

By Theorem 5.3 (i) this has a finite number of solutions with $\gcd(\alpha, \beta)$ square-free. In practice we compute these solutions by solving the S-unit equation $X + Y = 1$ over finitely many field extensions of K of degree at most 2 (see Theorem 5.3 (i)).

1.2 Our results

Our main theorem regarding the Asymptotic Fermat Last Theorem for signature $(p, p, 2)$ reads as follows:

Theorem 1.5 (Main Theorem for $(p, p, 2)$)**.** *Let K be a totally real number field and $S_K := \{\mathfrak{P} : \mathfrak{P}$ is a prime of K above $2\}$. Suppose $Cl_{S_K}(K)[2] = 1$. Moreover, define $U_{K,\mathfrak{P}} := \{(a, b, c) \in \mathcal{O}_K^3 : a^p + b^p = c^2$ with $\mathfrak{P}|b\}$, where $\mathfrak{P} \in S_K$ is a fixed prime.*
Suppose that there exists some distinguished prime $\tilde{\mathfrak{P}} \in S_K$, such that for every solution (α, β) to the S_K-unit equation:

$$\alpha + \beta = \gamma^2,\ \alpha, \beta \in \mathcal{O}_{S_K}^*,\ \gamma \in \mathcal{O}_{S_K}$$

it satisfies $|v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta})| \leq 6v_{\tilde{\mathfrak{P}}}(2)$.
Then, there is a B_K - depending only on K- such that for each rational prime $p > B_K$, the equation $a^p + b^p = c^2$ has no non-trivial , primitive solutions with $(a, b, c) \in U_{K,\tilde{\mathfrak{P}}}$ (i.e. the asymptotic Fermat holds for $U_{K,\tilde{\mathfrak{P}}}$).

Notation 1.6. Note that by Proposition 2.2 we allow ourselves to use $Cl_S(K)$ to mean $Cl(K)/\langle[\mathfrak{P}]\rangle_{\mathfrak{P}\in S}$ for S a finite set of primes of K and consequently, $Cl_S(K)[n]$ denotes its n-torsion points.

We use the same method involving modularity, lever lowering and image of inertia comparison to study the analogue asymptotic behaviour of the $(p, p, 3)$ equation and we get the following:

Theorem 1.7 (Main Theorem for $(p, p, 3)$)**.** *Let K be a totally real number field and $S_K := \{\mathfrak{P} : \mathfrak{P}$ is a prime of K above $3\}$. Suppose $Cl_{S_K}(K)[3] = 1$. Moreover, define $U_{K,\mathfrak{P}} := \{(a, b, c) \in \mathcal{O}_K^3 : a^p + b^p = c^3$ with $\mathfrak{P}|b\}$, where $\mathfrak{P} \in S_K$ is a fixed prime.*
Suppose that there exists some distinguished prime $\tilde{\mathfrak{P}} \in S_K$ such that for every solution (α, β) to the S_K-unit equation:

$$\alpha + \beta = \gamma^3,\ \alpha, \beta \in \mathcal{O}_{S_K}^*,\ \gamma \in \mathcal{O}_{S_K}$$

it satisfies $|v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta})| \leq 3v_{\tilde{\mathfrak{P}}}(3)$.
Then, there is a B_K - depending only on K- such that for each rational prime $p > B_K$, the equation $a^p + b^p = c^3$ has no non-trivial, primitive solutions with $(a, b, c) \in U_{K,\tilde{\mathfrak{P}}}$ (i.e. the asymptotic Fermat holds for $U_{K,\tilde{\mathfrak{P}}}$).

Remark 1.8. By Theorem 5.3 (ii) the S-unit equation $\alpha + \beta = \gamma^3$ has a finite number of solutions with $\gcd(\alpha, \beta)$ cube-free. In practice we compute these solutions by solving the S-unit equation $X + Y = 1$ over finitely many field extensions of K of degree at most 3 (see Theorem 5.3 (ii)).

We now answer the natural question of how these proofs differ from the proof of Theorem 1.1. The strategy is very similar, and requires a partial result towards the modularity conjecture for elliptic curves over totally real fields proved in [12] by Freitas, Hung and Siksek (discussed in Section 2.6). More precisely, the proof goes as follows. In each of the above main theorems, we assume the existence of a non-trivial, primitive solution (a, b, c). As in the rational case, we can assign a Frey elliptic curve E and prove that $\overline{\rho}_{E,p}$, its mod p Galois representation, is irreducible (Section 2.4). Then, we can use a result analogue to Ribet level lowering theorem to get a Hilbert eigenform $\mathfrak{f}$ of parallel weight 2 of lower level than the conductor of E. Here the modularity result in Section 2.3 gives an elliptic curve E' which has the same mod p Galois representation $\overline{\rho}_{E',p} \sim \overline{\rho}_{E,p}$.
We cannot use complex multiplication to get a contradiction as in the rational case. However, inspired by [14] and [21], we study the image of inertia subgroups $I_{\mathfrak{q}}$ (for certain primes $\mathfrak{q}$) under $\overline{\rho}_{E,p}$ and hence we get information about the action of $I_{\mathfrak{q}}$ on $E'[p]$. We use this to conclude that E' has good reduction outside even primes in Theorem 1.5 and outside primes dividing 3 in Theorem 1.7. To get a contradiction, we parametrize all of the possible elliptic curves E' by S-unit equations involving α, β and then make use of the action of $I_{\tilde{\mathfrak{P}}}$ to get information about $v_{\tilde{\mathfrak{p}}}(\frac{\alpha}{\beta})$. These valuations will lead to the contradictions which conclude the proofs.

1.3 Notational conventions

We will follow the notational conventions established by Siksek and Freitas in [14]. Throughout p denotes a rational prime, and K a totally real number field, with ring of integers $\mathcal{O}_K$. For a non-zero ideal I of $\mathcal{O}_K$, we denote by $[I]$ the class of I in the class group $\mathrm{Cl}(K)$.
Let $G_K = \mathrm{Gal}(\bar{K}/K)$. For an elliptic curve E/K, we write

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

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

2 Preliminaries

2.1 S-properties

In this section fix K a number field and let S be a finite set of prime ideals of K. As usual, $\mathrm{Cl}(K)$ is the class group of K.

We define the *ring of S-integers* and the *group of S-units* of K to be:

$$\mathcal{O}_{K,S} = \{x \in K : v_{\mathfrak{q}}(x) \geq 0, \forall\, \mathfrak{q} \notin S\}$$

$$\mathcal{O}^*_{K,S} = \{x \in K : v_{\mathfrak{q}}(x) = 0, \forall\, \mathfrak{q} \notin S\}$$

If the field K is understood from the context we just use $\mathcal{O}_S, \mathcal{O}^*_S$ respectively. We observe that $\mathcal{O}^*_{K,S}$ is the group of units of $\mathcal{O}_{K,S}$. One can show that $\mathcal{O}_{K,S}$ is a Dedekind domain and $\mathcal{O}^*_{K,S}$ is finitely generated abelian group. The generators of $\mathcal{O}^*_{K,S}$ can be chosen to be algebraic integers and $\mathcal{O}^*_{K,S}$ decomposes as:

$$\mathcal{O}^*_{K,S} = \mathcal{O}^*_K \oplus \bigoplus_{i=1}^{\#S} \mathbb{Z}\gamma_i \tag{2}$$

with $\gamma_i \notin \mathcal{O}^*_K$.

Remark 2.1. Identity (2) together with Dirichlet's Unit Theorem (see [6] for an insightful survey of this) give an explicit way to compute the generators of $\mathcal{O}^*_{K,S}$. Moreover, this is implemented in various mathematics softwares (e.g. Sage).

We say that an ideal I of K is *S-integral* if $v_{\mathfrak{q}}(I) \geq 0$ for all $\mathfrak{q} \notin S$ and that is an *S-ideal* if $v_{\mathfrak{q}}(I) = 0$ for all $\mathfrak{q} \notin S$. We define the *S-class group* $Cl_S(K)$ to be the class group of $\mathcal{O}_{K,S}$.

Proposition 2.2. *There is a canonical isomorphism:*

$$Cl_S(K) \simeq Cl(K)/\langle[\mathfrak{P}]\rangle_{\mathfrak{P}\in S}$$

where $\langle[\mathfrak{P}]\rangle_{\mathfrak{P}\in S}$ is the subgroup of $Cl(K)$ generated by the images of $\mathfrak{P}$ in $Cl(K)$.

Proof. See [4], Proposition 7.4.4. □

For a positive natural integer n we denote the *n-Selmer group* of K and S to be

$$K(S,n) = \{x \in K^*/(K^*)^n : v_{\mathfrak{P}}(x) \equiv 0 \mod n, \forall \mathfrak{P} \notin S\}$$

The *n-Kummer exact sequnce* of $\mathcal{O}^*_{K,S}$ holds:

$$1 \longrightarrow \mathcal{O}^*_{K,S}/(\mathcal{O}^*_{K,S})^n \longrightarrow K(S,n) \xrightarrow{a_n} \mathrm{CL}_S(K)[n] \longrightarrow 1 \tag{3}$$

where $\mathrm{CL}_S(K)[n]$ is the n-torsion subgroup of $\mathrm{CL}_S(K)$ and the map $a_n \colon K(S,n) \to \mathrm{CL}_S(K)[n]$ is given by $x \to [I_S]$ such that $(x)\mathcal{O}_{K,S} = I_S^n$.

2.2 Elliptic Curves

We begin by collecting some useful results about elliptic curves, as they play a key role in the modular approach of solving Diophantine equations.

Lemma 2.3. *Let K be a field of $char(K) \neq 2, 3$ and E/K an elliptic curve. The following holds:*

(i) If E has a K-rational point of order 2, then E can has a model of the form

$$E : Y^2 = X^3 + aX^2 + bX. \tag{4}$$

Moreover, there is a bijection between

$$\{E/K \text{ with a } K\text{-torsion of order } 2 \text{ up to } \bar{K}-\text{isomorphism}\} \longmapsto \mathbb{P}^1(K)-\{4, \infty\}$$

via the map $E \longmapsto \lambda := \frac{a^2}{b}$.

(ii) If E has a K-rational point of order 3, then E has a model of the form

$$E : Y^2 + cXY + dY = X^3. \tag{5}$$

Moreover, there is a bijection between

$$\{E/K \text{ with a } K\text{-torsion of order } 3 \text{ up to } \bar{K}-\text{isomorphism}\} \longmapsto \mathbb{P}^1(K)-\{27, \infty\}$$

via the map $E \longmapsto \lambda := \frac{c^3}{d}$.

Proof. (i) Any elliptic curve E in the Weirstrass form over a field K of $\text{char}(K) \neq 2$ can be turned into:

$$E : Y^2 = X^3 + aX^2 + bX + c$$

after a change of variables, see [30] (III.1) for details. Now, the K-torsion point of order 2 can be moved via a translation to the point $(0, 0)$, giving the desired form: $E : Y^2 = X^3 + aX^2 + bX$. As $(0, 0) + (0, 0) = \infty$, under the group law, we are done. See [30] (III.2) for an explicit group law algorithm.

For the second part, we are given an elliptic curve E/K with a K-torsion point of order 2. After writing it as in (4), we make the assignment $E \mapsto \lambda := \frac{a^2}{b}$. As $\Delta_E = 2^4b^2(a^2 - 4b)$, non-singularity of E gives $\lambda \in \mathbb{P}^1(K) - \{4, \infty\}$, which proves our map is well-defined. Moreover, any $\lambda \in \mathbb{P}^1(K) - \{4, \infty\}$ can be written as a ratio of the form $\frac{a^2}{b}$ with $b \neq 0$ and $a^2 \neq 4b$, and hence comes from an elliptic curve with a K-rational 2-torsion. Thus, our map is surjective.
Injectivity follows from writing

$$j_E = 2^8 \frac{(a^2 - 3b)^3}{b^2(a^2 - 4b)} = 2^8 \frac{(\lambda - 3)^3}{\lambda - 4}$$

and noting that $\lambda = \lambda'$ for given $E \to \lambda$, $E' \to \lambda'$ implies $j_E = j_{E'}$, which gives $E \simeq E'$.

(ii) Again, if E is in Weirstrass form we can translate the K-torsion point to $(0,0)$. This will give a model of the form:

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X$$

As before, explicit computations can be found in [30] (III.1). We now impose the condition that $(0,0)$ has order 3. First, we compute $-(0,0) = (0,-a_3)$ and note that we require $(0,0) \neq -(0,0) = (0,-a_3)$ (see [30] (III.2) for an explicit group law algorithm), so $a_3 \neq 0$. Now, by performing the change of variables:

$$\begin{cases} Y \to (Y + \frac{a_4}{a_3}X) \\ X \to X \end{cases} \tag{6}$$

we get a model of the form:

$$E : Y^2 + cXY + dY = X^3 + eX^2 \text{ with } d = a_3 \neq 0.$$

Finally, we make use of the order 3 again and rules of adding points on E, as given in [30] (III.2):

$$\begin{cases} (0,0) + (0,0) = -(0,0) = (0,-d) \\ (0,0) + (0,0) = (-e,-d) \end{cases} \tag{7}$$

Hence, we need $e = 0$, and we get the desired form: $E : Y^2 + cXY + dY = X^3$.

For the second part, we are given an elliptic curve E/K with a K-torsion point of order 3. After writing it as in (5), we make the assignment $E \mapsto \lambda := \frac{c^3}{d}$. As $\Delta_E = d^3(c^3 - 27d)$, non-singularity of E gives $\lambda \in \mathbb{P}^1(K) - \{27, \infty\}$, which proves our map is well-defined. Moreover, any $\lambda \in \mathbb{P}^1(K) - \{27, \infty\}$ can be written as a ratio of the form $\frac{c^3}{d}$ with $d \neq 0$ and $c^3 \neq 27d$, and hence comes from an elliptic curve with a K-rational 3-torsion. Thus, our map is surjective.
Injectivity follows from writing

$$j_E = \frac{c^3(c^3 - 24d)^3}{d^3(c^3 - 27d)} = \frac{\lambda(\lambda - 24)^3}{\lambda - 27}$$

and noting that $\lambda = \lambda'$ for given $E \to \lambda$, $E' \to \lambda'$ implies $j_E = j_{E'}$, which gives $E \simeq E'$.

□

Lemma 2.4. *Let K be a number field and S a set of finite primes of K. Then:*

(i) If S contains the primes above 2 we get the following bijection $\left\{\begin{matrix}E/K \text{ with a } K\text{-torsion of order 2 with potentially} \\ \text{good reduction outside } S \text{ up to } \bar{K}\text{-isomorphism}\end{matrix}\right\} \longmapsto \mathcal{O}_S^*$ *via the map $E \longmapsto \mu := \lambda - 4 \in \mathcal{O}_S^*$, where λ is as in Lemma 2.3 (i).*

(ii) If S contains the primes above 3 we get the following bijection $\left\{\begin{matrix}E/K \text{ with a } K\text{-torsion of order 3 with potentially} \\ \text{good reduction outside } S \text{ up to } \bar{K}\text{-isomorphism}\end{matrix}\right\} \longmapsto \mathcal{O}_S^*$ *via the map $E \longmapsto \mu := \lambda - 27 \in \mathcal{O}_S^*$, where λ is as in Lemma 2.3 (ii).*

Proof. (i) Let E be an elliptic curve with a K-torsion point of order 2 with potentially good reduction outside S. By Lemma 2.3 (i) E has a model:

$$E : Y^2 = X^3 + aX^2 + bX$$

with $\lambda := \frac{a^2}{b}$ and $\mu := \lambda - 4 = \frac{a^2-4b}{b}$. Thus,

$$j_E = 2^8 \frac{(\lambda - 3)^3}{\lambda - 4} = 2^8 \frac{(\mu + 1)^3}{\mu}. \tag{8}$$

Good reduction outside S implies that $v_{\mathfrak{q}}(j_E) \geq 0$ for all $\mathfrak{q} \notin S$, in other words $j_{E'} \in \mathcal{O}_S$.

Consequently both λ and μ satisfy monic equations with coefficients in $\mathcal{O}_S$. Thus, we can conclude that $\lambda, \mu \in \mathcal{O}_S$. Moreover, by writing j_E in terms of μ^{-1} and using the same reasoning, we deduce that also $\mu^{-1} \in \mathcal{O}_S$ and hence $\mu \in \mathcal{O}_S^*$ and so the assignment $E \longmapsto \mu$ is well-defined.
Note that every $\mu \in \mathcal{O}_S^*$ can be written in the form $\mu = \frac{a^2}{b} - 4$ for some $a, b \in K$, thus coming from an elliptic curve with 2-torsion. Moreover, $\mu \in \mathcal{O}_S^*$ implies $j_E \in \mathcal{O}_S$, thus this represents a curve with potentially good reduction outside S, proving surjectivity.
Injectivity follows by noting that $\mu = \mu'$ implies $j_E = j'_E$ which gives $E \simeq E'$..

(ii) Let E be an elliptic curve with a K-torsion point of order 3 with potentially good reduction outside S. By Lemma 2.3 (ii) E has a model:

$$E : Y^2 + cXY + dY = X^3$$

with $\lambda := \frac{c^3}{d}$ and $\mu = \lambda - 27 = \frac{c^3 - 27d}{d}$ Thus,

$$j_E = \frac{\lambda(\lambda-24)^3}{\lambda-27} = \frac{(\mu+27)(\mu+3)^3}{\mu}. \tag{9}$$

Same arguments as in the proof of (i) give $j_E, \lambda \in \mathcal{O}_S$ and $\mu \in \mathcal{O}_S^*$, giving $E \longmapsto \mu$ is well-defined.
Surjectivity and injectivity follow exactly as in (i).

□

Lemma 2.5. *Let K be a number field and S a set of finite primes of K. Let E/K be an elliptic curve with good reduction outside S.*

(i) If S contains the primes above 2 and E has a K-torsion point of order 2, we get by Lemma 2.4 (i) an equation $\lambda - \mu = 4$ with $\lambda \in \mathcal{O}_S$, $\mu \in \mathcal{O}_S^*$ depending on the coefficients of E.
Moreover, good reduction gives the ideal relation $(\lambda)\mathcal{O}_K = I^2 J$ where J is an S-ideal.

(ii) If S contains the primes above 3 and E has a K-torsion point of order 3, we get by Lemma 2.4 (ii) an equation $\lambda - \mu = 27$ with $\lambda \in \mathcal{O}_S$, $\mu \in \mathcal{O}_S^*$ depending on the coefficients of E.
Moreover, good reduction gives the ideal relation $(\lambda)\mathcal{O}_K = I^3 J$ where J is an S-ideal.

Proof. (i) By Lemma 2.3 (i) E has a model:

$$E : Y^2 = X^3 + aX^2 + bX$$

with $\Delta_E = 2^4 b^2(a^2 - 4b)$ and $c_4 = 2^4(a^2 - 3b)$. Good reduction outside S implies that for a $\mathfrak{q} \notin S$ we have that $v_\mathfrak{q}(\Delta_{\min}) = 0$ (where $\Delta_{\min}$ is the minimal discriminant of E viewed over the local field $K_\mathfrak{q}$). So, $\mathfrak{q}^{12k} || \Delta_E$ and $\mathfrak{q}^{4k} | c_4$ for some integer k. This follows from standard results about minimal discriminants of elliptic curves which can be found in [30] VII.1. Therefore, $\mathfrak{q}^{2k} | a$ and $\mathfrak{q}^{4k} || b$. Hence,

$$(a)\mathcal{O}_K = \prod_{\mathfrak{q} \notin S_K} \mathfrak{q}^{4k_\mathfrak{q} + 2l_\mathfrak{q}} \prod_{\mathfrak{P} \in S_K} \mathfrak{P}^{a_\mathfrak{P}},\ (b)\mathcal{O}_K = \prod_{\mathfrak{q} \notin S_K} \mathfrak{q}^{4k_\mathfrak{q}} \prod_{\mathfrak{P} \in S_K} \mathfrak{P}^{b_\mathfrak{P}}.$$

Thus, as $\lambda = \frac{a^2}{b}$, we get:

$$(\lambda)\mathcal{O}_K = I^2 J, \text{ where } I := \prod_{\mathfrak{q} \notin S_K} \mathfrak{q}^{l_\mathfrak{q}},\ J := \prod_{\mathfrak{P} \in S_K} \mathfrak{P}^{2a_\mathfrak{P} - b_\mathfrak{P}}.$$

which makes J an S-ideal.

(ii) By Lemma 2.3 (ii) E has a model:

$$E : Y^2 + cXY + dY = X^3$$

with $\Delta_E = d^3(c^3 - 27d)$ and $c_4 = c(c^3 - 24d)$. Good reduction outside S implies that for a $\mathfrak{q} \notin S$ we have that $v_{\mathfrak{q}}(\Delta_{\min}) = 0$ (where $\Delta_{\min}$ is the minimal discriminant of E viewed over the local field $K_{\mathfrak{q}}$). So, $\mathfrak{q}^{12k} || \Delta_E$ and $\mathfrak{q}^{4k} | c_4$ for some integer k. This follows from standard results about minimal discriminants of elliptic curves which can be found in [30] VII.1. Therefore, $\mathfrak{q}^{3k} | d$ and $\mathfrak{q}^k || c$. Hence,

$$(c)\mathcal{O}_K = \prod_{\mathfrak{q} \notin S} \mathfrak{q}^{k_{\mathfrak{q}} + l_{\mathfrak{q}}} \prod_{\mathfrak{P} \in S} \mathfrak{P}^{c_{\mathfrak{P}}}, \ (d)\mathcal{O}_K = \prod_{\mathfrak{q} \notin S} \mathfrak{q}^{3k_{\mathfrak{q}}} \prod_{\mathfrak{P} \in S} \mathfrak{P}^{d_{\mathfrak{P}}}.$$

Thus, as $\lambda = \frac{c^3}{d}$, we get:

$$(\lambda)\mathcal{O}_K = I^3 J, \text{ where } I := \prod_{\mathfrak{q} \notin S} \mathfrak{q}^{l_{\mathfrak{q}}}, \ J := \prod_{\mathfrak{P} \in S} \mathfrak{P}^{3c_{\mathfrak{P}} - d_{\mathfrak{P}}}.$$

which makes J an S-ideal.

□

2.3 Modularity Results

It is perhaps not surprising that the modular approach for Diophantine equations over totally real fields involves some adaptation of the classical modularity theorem over the rationals.
Let's first recall that given K a totally real number field, G_K its absolute Galois group and E an elliptic curve over K, we say that E is *modular* if there exists a Hilbert cuspidal eigenform $\mathfrak{f}$ over K of parallel weight 2, with rational Hecke eigenvalues, such that the Hasse–Weil L-function of E is equal to the Hecke L-function of $\mathfrak{f}$. A more conceptual way to phrase this is that there is an isomorphism of compatible systems of Galois representations

$$\rho_{E,p} \simeq \rho_{\mathfrak{f},p}$$

where the left-hand side is the Galois representation arising from the action of G_K on the p-adic Tate module $T_p(E)$, while the right-hand side is the Galois representation associated to $\mathfrak{f}$. A comprehensive definition of *Hilbert modular forms* and their associated representation can be found, for example in Wiles' [37].
We will need the following remarkable theorem proved by Freitas, Hung and Siksek in [12]:

Theorem 2.6. *Let K be a totally real field. Up to isomorphism over $\bar{K}$, 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.*

Furthermore Derickx, Najman and Siksek have recently proved in [10]:

Theorem 2.7. *Let K be a totally real cubic number field and E be an elliptic curve over K. Then E is modular.*

2.4 Irreductibility of $\bmod p$ representations of elliptic curves

We need the following theorem in the lever lowering step of our proof. This was proved in [13] as Theorem 2 and it is derived from the work of David, Momose who in turn built on Merel's Uniform Boundedness Theorem.

Theorem 2.8. *Let K be a Galois totally real field. There is an effective constant C_K, depending only on K, such that the following holds. If $p > C_K$ is prime, and E is an elliptic curve over K which has multiplicative reduction at all $\mathfrak{q}|p$, then $\overline{\rho}_{E,p}$ is irreducible.*

2.5 Level lowering

We present a lever lowering result proved by Freitas and Siksek in [14] derived from the work of Fujira [15], Jarvis[17], and Rajaei[24]. 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:

$$\mathcal{M}_p = \prod_{\substack{\mathfrak{q}||\mathcal{N}_E \\ p|v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})}} \mathfrak{q}, \text{ and } \mathcal{N}_p = \frac{\mathcal{N}_E}{\mathcal{M}_p} \tag{10}$$

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 2.9. *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) $p|v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$ *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 $\overline{\omega}$ of $\mathbb{Q}_{\mathfrak{f}}$ such that $\overline{\omega}|p$ and $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\overline{\omega}}$.

Proof. We give a sketch of the proof as described in [14] for completion, using the theorems in [15], [17] and [24]. Assumption (i) takes care of some technical restrictions in those theorems.
By assumption (ii), there is a newform $\mathfrak{f}_0$ of parallel weight 2, level $\mathcal{N}$ and field of coefficients $\mathbb{Q}_{\mathfrak{f}_0} = \mathbb{Q}$, such that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f}_0,p}$. Thus $\overline{\rho}_{E,p}$ is modular, and by (iii) is irreducible. Since K may be of even degree, in order to apply the main result of [24], we need to add an auxiliary (special or supercuspidal) prime to the level. From [24], Theorem 5 we can add an auxiliary (special) prime $\mathfrak{q}_0 \nmid \mathcal{N}$ so that $\overline{\rho}_{\mathfrak{f}_0,p}(\sigma_{\mathfrak{q}_0})$ is conjugate to $\overline{\rho}_{\mathfrak{f}_0,p}(\sigma)$, where $\sigma_{\mathfrak{q}_0}$ denotes a Frobenius element of G_K at $\mathfrak{q}_0$ and σ is complex conjugation. We now apply the main theorem of [24] to remove from the level all primes $\mathfrak{q} \nmid \mathfrak{p}$ dividing $\mathcal{M}_p$. Next we remove from the level the primes above p without changing the weight. By [17], Theorem 6.2 we can do this provided $\overline{\rho}_{E,p}G_{\mathfrak{q}}$ is finite at all $\mathfrak{q}|\mathfrak{p}$, where $G_{\mathfrak{q}}$ is the decomposition subgroup of $G + K$ at $\mathfrak{q}$. But from (iv), $\mathfrak{q}$ is a prime of good or multiplicative reduction for E. In the former case, $\overline{\rho}_{E,p}|G_{\mathfrak{q}}$ is finite; in the latter case it is finite by (v). Finally, from the condition imposed on $\mathfrak{q}_0$ it follows that $\mathrm{Norm}(\mathfrak{q}_0) \not\equiv 1(\mod p)$, and we can apply Fujiwara's version of Mazur's principle [15] to remove $\mathfrak{q}_0$ from the level. We conclude that there is an eigenform $\mathfrak{q}$ of parallel weight 2, new at level $\mathcal{N}_p$, and a prime $\bar{\omega}|p$ of $\mathbb{Q}_{\mathfrak{f}}$ such that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f}_0,p} \sim \overline{\rho}_{\mathfrak{f},\bar{\omega}}$.

□

2.6 Eichler-Shimura

We would like to use the following:

Conjecture 2.10 (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 rational eigenvalues. Then there is an elliptic curve $E_{\mathfrak{f}}/K$ with conductor $\mathcal{N}$ having the same L-function as $\mathfrak{f}$.

However, we do not have a proof for this yet, but the following partial result holds:

Theorem 2.11. *Let K be a totally real field and let $\mathfrak{f}$ be a Hilbert newform over K of level $\mathcal{N}$ and parallel weight 2, such that $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. Suppose that:*

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

(ii) or there is a finite prime $\mathfrak{q}$ such that 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 $\mathfrak{f}$.

Proof. This was derived by Blasius in [3] from the work of Hilda for a more general (ii). For the particular case that we use, the proof was given by Darmon [7] and Zhang [39]. □

Freitas and Siksek obtain the following corollary from the above theorem in [14].

Corollary 2.12. *Let E be an elliptic curve over a totally real fiel K , and p be an odd prime. Suppose that $\overline{\rho}_{E,p}$ is irreducible, and $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\overline{\omega}}$ 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:*

(i) E has potentially multiplicative reduction at $\mathfrak{q}$;

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

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

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

Proof. We will give the proof as in [14] for completion.
Write c_4 and c_6 for the usual c-invariants of E, which are non-zero as E has potentially multiplicative reduction at $\mathfrak{q}$. Let $\gamma = -c_4/c_6$. Write χ for the quadratic character associated to $K(\sqrt{\gamma})/K$ and $E \otimes \chi$ for the γ-quadratic twist of E.
By [31] Theorem V.5.3, $E \otimes \chi$ has split multiplicative reduction at $\mathfrak{q}$. Let $\mathfrak{g} = \mathfrak{f} \otimes \chi$. As χ is quadratic and $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$ it follows that $\mathbb{Q}_{\mathfrak{g}} = \mathbb{Q}$.
Suppose $\mathfrak{g}$ is new at some level $\mathcal{N}_{\mathfrak{g}}$. We will prove $v_{\mathfrak{q}}(\mathcal{N}_{\mathfrak{g}}) = 1$. Then, by Theorem 2.11 there is some elliptic curve $E_{\mathfrak{g}}$ having the same L-function as $\mathfrak{g}$. Thus, the L-functions of $E_{\mathfrak{g}} \otimes \chi$ and $\mathfrak{q} \otimes \chi = f$ are equal, and we take $E_{\mathfrak{f}} = E_{\mathfrak{g}} \otimes \chi$.
It remains to prove that $v_{\mathfrak{q}}(\mathcal{N}_{\mathfrak{g}}) = 1$. Since $\overline{\rho}_{E\otimes\chi,p} \sim \overline{\rho}_{\mathfrak{g},p}$, the two representations have the same optimal Serre level $\mathfrak{R}$ (say). Now $E \otimes \chi$ has multiplicative reduction at $\mathfrak{q}$, so $v_{\mathfrak{q}}(\mathfrak{R}) = 0$ or 1. Since E and $E \otimes \chi$ are isomorphic over $K(\gamma)$, and as $p | \#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$, we have $p | \#\overline{\rho}_{E\otimes\chi,p}(I_{\mathfrak{q}})$, hence $v_{\mathfrak{q}}(\mathfrak{R}) \neq 0$ so $v_{\mathfrak{q}}(\mathfrak{R}) = 1$.
We now think of $\mathfrak{R}$ as the optimal Serre level at $\overline{\rho}_{\mathfrak{q},p}$ and compare it to the level $\mathcal{N}_{\mathfrak{g}}$ of $\mathfrak{g}$. By [16] Theorem 1.5, $v_{\mathfrak{q}}(\mathcal{N}_{\mathfrak{q}}) = v_{\mathfrak{q}}(\mathfrak{R})$ except possibly when $v_{\mathfrak{q}}(\mathcal{N}_{\mathfrak{q}}) = 1$ and $v_{\mathfrak{q}}(\mathfrak{R} = 0$ or when $\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{q}) = \pm 1 (\mod p)$. The former is impossible as $v_{\mathfrak{q}}(\mathfrak{R}) = 1$ and the latter is ruled out by (iii). Thus $v_{\mathfrak{q}}(\mathcal{N}_{\mathfrak{g}}) = 1$.

□

3 Proof of Main Theorem for signature $(p, p, 2)$

This section is dedicated to proving Theorem 1.5. Let K be a totally real field. Recall the sets:

$$S_K = \{\mathfrak{P} \ : \mathfrak{P} \text{ is a prime of } K \text{ above } 2\}$$

$U_{K,\mathfrak{P}} = \{(a, b, c) \in \mathcal{O}_K^3 : a^p + b^p = c^2 \text{ with } \mathfrak{P} | b\}$, where $\mathfrak{P} \in S_K$ is a fixed prime.

3.1 Frey Curve

For a non-trivial, primitive solution (a, b, c) of $a^p + b^p = c^2$ we associate the following Frey elliptic curve defined over K:

$$E : Y^2 = X^3 + 4cX^2 + 4a^pX. \tag{11}$$

We use [30] (III.1) to compute the arithmetic invariants:

$$\Delta_E = 2^{12}(a^2b)^p, c_4 = 2^6(4b^p + a^p) \text{ and } j_E = 2^6\frac{(4b^p + a^p)^3}{(a^2b)^p}.$$

Lemma 3.1. *Let (a, b, c) be the non-trivial, primitive solution to the equation $a^p + b^p = c^2$. Let E be the associated Frey curve (11) with conductor $\mathcal{N}_E$. Then, for all primes $\mathfrak{q} \notin S_K$, the model E is minimal, semistable and satisfies $p|v_\mathfrak{q}(\Delta_E)$. Moreover*

$$\mathcal{N}_E = \prod_{\mathfrak{P}\in S_K} \mathfrak{P}^{r_\mathfrak{P}} \prod_{\substack{\mathfrak{q}|ab \\ \mathfrak{q}\notin S_K}} \mathfrak{q}, \ \mathcal{N}_p = \prod_{\mathfrak{P}\in S_K} \mathfrak{P}^{r'_\mathfrak{P}} \tag{12}$$

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

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. In particular, $v_\mathfrak{q}(c_4) < 4$ and as the coefficients of E are in $\mathcal{O}_K$ we can use [30] VII.1 Remark 1.1. to deduce that the model is minimal at q and [30] VII.5. Proposition 5.1. to deduce that E has multiplicative reduction at $\mathfrak{q}$ as $v_\mathfrak{q}(\Delta_E) > 0$ and $v_\mathfrak{q}(c_4) = 0$. Hence $p|v_\mathfrak{q}(\Delta_E) = v_\mathfrak{q}(\Delta_\mathfrak{q})$. On the other hand, if $\mathfrak{P} \in S_K$, an even prime, we have $r_\mathfrak{P} = v_\mathfrak{P}(\mathcal{N}_E) \leq 2 + 6v_\mathfrak{P}(2)$ by [31] Theorem IV.10.4. The definition of $\mathcal{N}_E$ gives the desired form in (12). Then, use (10) to get $\mathcal{N}_p$ and observe that $r'_\mathfrak{P} = r_\mathfrak{P}$ unless E has multiplicative reduction at $\mathfrak{P}$ and $p|v_\mathfrak{P}(\Delta_\mathfrak{P})$ in which case $r_\mathfrak{P} = 1$ and $r'_\mathfrak{P} = 0$. □

Lemma 3.2. *Let K be a totally real field. There is some constant A_K depending only on K, such that for any non-trivial, primitive solution (a, b, c) of $a^p + b^p = c^2$ and $p > A_K$, the Frey curve given by (11) is modular.*

Proof. By Theorem 2.6, there are at most finitely many possible $\bar{K}$-isomorphism classes of elliptic curves over E which are not modular. Let $j_1, j_2, \ldots, j_n \in K$ be the j-invariants of these classes. Define $\lambda := b^p/a^p \notin \{0, \pm 1\}$ (as a, b are non-trivial and coprime). The j-invariant of E is

$$j(\lambda) = 2^6(4\lambda + 1)^3\lambda^{-1}.$$

Each equation $j(\lambda) = j_i$ has at most three solutions $\lambda \in K$. Thus there are values $\lambda_1, \ldots, \lambda_m \in K (m \leq 3n)$ such that if $\lambda \neq \lambda_k$ for all k, then the

elliptic curve E with j-invariant $j(\lambda)$ is modular.
If $\lambda = \lambda_k$ then $(b/a)^p = \lambda_k$, but the polynomial $x^p + \lambda_k$ has a root in K if and only if $\lambda_k \in (K^*)^p$ because K is totally real and $\lambda_k \notin \{0, \pm 1\}$. Hence we get a lower bound on p for each k, and by taking the maximum of these bounds we get A_K.

Remark 3.3. The constant A_K is ineffective as the finiteness of Theorem 2.6 relies on Falting's Theorem (which is ineffective). See [12] for more details. Note that if K is quadratic or cubic we get $A_K = 0$ (by the last part of Theorem 2.6 and Theorem 2.7).

□

3.2 Images of Inertia

We gather information about the images of inertia $\overline{\rho}_{E,p}(I_\mathfrak{q})$. This is a crucial step in applying Corollary 2.12 and for controlling the behaviour at the primes in S_K of the newform obtained by level lowering.

Lemma 3.4. *Let E be an elliptic curve over K with j-invariant j_E. Let $p \geq 5$ and let $\mathfrak{q} \nmid p$ 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. $v_\mathfrak{q}(j_E) < 0$) and $p \nmid v_\mathfrak{q}(j_E)$.*

Proof. See [14] Lemma 3.4. □

Lemma 3.5. *Let $\mathfrak{q} \nmid 2$ and let (a, b, c) be a non-trivial, primitive solution to the equation $a^p + b^p = c^2$ with the prime exponent $p \geq 5$, such that $\mathfrak{q} \nmid p$. Let E be the Frey curve in (11). Then $p \nmid \#\overline{\rho}_{E,p}(I_\mathfrak{q})$.*

Proof. Using Lemma 3.4, it is enough to show that at all $\mathfrak{q} \nmid 2$ and $\mathfrak{q} \nmid p$ either $v_\mathfrak{q}(j_E) \geq 0$ or $p | v_\mathfrak{q}(j_E)$. If $\mathfrak{q} \nmid \Delta_E$, then E has good reduction at $\mathfrak{q}$, so $v_\mathfrak{q}(j_E) \geq 0$. 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. $v_\mathfrak{q}(c_4) = 0$. Thus, $v_q(j_E) = -p v_\mathfrak{q}(a^2 b)$, i.e. $p | v_\mathfrak{q}(j_E)$. □

Lemma 3.6. *Let $\mathfrak{P} \in S_K$ and $(a, b, c) \in U_{K,\mathfrak{P}}$ non-trivial, primitive with prime exponent $p > 6 v_\mathfrak{P}(2)$. Let E be the Frey curve in (11) with j-invariant j_E. Then E has potentially multiplicative reduction at $\mathfrak{P}$ and $p | \#\overline{\rho}_{E,p}(I_\mathfrak{P})$.*

Proof. Assume that $\mathfrak{P} \in S_K$ with $v_\mathfrak{P}(b) = k$. Then $v_\mathfrak{P}(j_E) = 6 v_\mathfrak{P}(2) - pk$. Since $p > 6 v_\mathfrak{P}(2)$, it follows that $v_\mathfrak{P}(j_E) < 0$ and clearly $p \nmid v_\mathfrak{P}(j_E)$. This implies that E has potentially multiplicative reduction at $\mathfrak{P}$ and by Lemma 3.4 we get $p | \#\overline{\rho}_{E,p}(I_\mathfrak{P})$. □

3.3 Lever Lowering and Eichler Shimura

This is a key result in the proof of Theorem 1.5, for which we have prepared the ingredients in the previous sections. We will follow the corresponding proofs in [14] and [21].

Theorem 3.7. *Let K be a totally real number field and assume it has a distinguished prime $\tilde{\mathfrak{P}} \in S_K$. Then there is a constant B_K depending only on K such that the following hold. Let $(a,b,c) \in U_{K,\tilde{\mathfrak{P}}}$ non-trivial, primitive with prime exponent $p > B_K$. Write E for the Frey curve (11). Then, there is an elliptic curve E' over K such that:*

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

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

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

(iv) E' has multiplicative reduction at $\tilde{\mathfrak{P}}$ ($v_{\tilde{\mathfrak{P}}}(j_{E'}) < 0$ where $j_{E'}$ is the j-invariant of E').

Proof. We first observe that by Lemma 3.1 that E has multiplicative reduction outside S_K. By taking B_K sufficiently large, we see from Lemma 3.2 that E is modular and by Theorem 2.8 that $\overline{\rho}_{E,p}$ is irreducible. Applying Theorem 2.9 and Lemma 3.1 we see that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\overline{\omega}}$ for a Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}_p$ and some prime $\overline{\omega}|p$ of $\mathbb{Q}_\mathfrak{f}$. Here $\mathbb{Q}_\mathfrak{f}$ denotes the field generated by the Hecke eigenvalues $\mathfrak{f}$.
Next we reduce to the case when $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$, after possibly enlarging B_K. This step uses standard ideas originally due to Mazur that can be found in [2] Section 4, [5] Proposition 15.4.2., and so we omit the details.
Next we want to show that there is some elliptic curve E'/K of conductor $\mathcal{N}_p$ having the same L-function as $\mathfrak{f}$.
We apply Lemma 3.6 with $\mathfrak{P} = \tilde{\mathfrak{P}}$ and get that E has potentially multiplicative reduction at $\tilde{\mathfrak{P}}$ and $p|\#\overline{\rho}_{E,p}(I_\mathfrak{P})$. The existence of E' follows from Corollary 2.12 after possibly enlarging B_K to ensure that $p \nmid (\mathrm{Norm}_{K/\mathbb{Q}}(\tilde{\mathfrak{P}}) \pm 1)$.
By putting all the pieces together we can conclude that there is an elliptic curve E'/K of conductor $\mathcal{N}_p$ satisfying $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$. This proves (i) and (ii).
We now want to show that we can choose E' such that it has a K-rational point of order 2. We will sketch the argument and refer the reader to [26] Section IV-6 for the details of the various equivalences involved. Note that since E has a K-rational point of order 2, then $2|\#\mathrm{Tors}(E(K))$ which implies that $2|\#E(\mathbb{F}_\mathfrak{q})$ for all primes $\mathfrak{q}$ at which E has good reduction. This is in turn equivalent to the fact that for all $s \in \mathrm{Im}(\overline{\rho}_{E,2})$, $\det(1-s) \equiv 0 \mod 2$. By (ii) we know $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$, so for all $s \in \mathrm{Im}(\overline{\rho}_{E',2})$, $\det(1-s) \equiv 0 \mod 2$. This is equivalent to the existence of an elliptic curve E'' with a K-rational point of order 2 which is either isomorphic to E' or it is 2-isogenous to E'.

So, by possibly replacing E' by E'' we get (iii).
Now let $j_{E'}$ be the j-invariant of E'. As we have already seen, Lemma 3.6 implies $p|\#\overline{\rho}_{E,p}(I_{\tilde{\mathfrak{P}}})$, hence $p|\#\overline{\rho}_{E',p}(I_{\tilde{\mathfrak{P}}})$, thus by Lemma 3.4 we get that E' has multiplicative reduction at $\tilde{\mathfrak{P}}$ and so $v_{\tilde{\mathfrak{P}}}(j_{E'}) < 0$. □

3.4 Proof of the Main Theorem

Proof. So far, we have shown that for a primitive, non-trivial solution $(a, b, c) \in U_{K,\tilde{\mathfrak{P}}}$ with a prime exponent p we associate the Frey elliptic curve in (11). By Theorem 3.7 for $p > B_K$ we can find an elliptic curve E' which is related to E by $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$ and has a K-rational point of order 2. Hence by Theorem 2.3 (i) we get a model:

$$E' : Y^2 = X^3 + a'X^2 + b'X$$

with arithmetic invariants $\Delta_{E'} = 2^4 b'^2(a'^2 - 4b')$, $j_{E'} = 2^8 \frac{(a'^2-3b')^3}{b'^2(a'^2-4b')}$.
Moreover, by Theorem 3.7 (i), we know that E' has good reduction outside S_K which implies that $v_{\mathfrak{q}}(j_{E'}) \geq 0$ for $\mathfrak{q} \notin S_K$. Therefore, $j_{E'} \in \mathcal{O}_{S_K}$. Consider $\lambda := \frac{a'^2}{b'}$ and $\mu := \lambda - 4 = \frac{a'^2-4b'}{b'}$. Next, we need to show that λ can be written as $\lambda = u\gamma^2$, where u is an S_K-unit.
By Lemma 2.5 (i) applied to E' we get that

$$(\lambda)\mathcal{O}_K = I^2 J \text{ where } J \text{ is an } S\text{-ideal.}$$

Thus $[I]^2 = [J]$ as elements of the class group $\mathrm{Cl}(K)$ and $[J] \in \langle[\mathfrak{P}]\rangle_{\mathfrak{P}\in S_K}$. This implies that $[I] \in Cl_{S_K}(K)[2]$ and by our assumption on K that $Cl_{S_K}(K)[2]$ is trivial, we get that $[I] \in \langle[\mathfrak{P}]\rangle_{\mathfrak{P}\in S_K}$, i.e. $I := \gamma\tilde{I}$, where $\tilde{I}$ is an S-ideal and $\gamma \in \mathcal{O}_K$. Consequently,

$$(\lambda)\mathcal{O}_K = (\gamma)^2\tilde{I}^2 J \text{ where both } \tilde{I} \text{ and } J \text{ are } S\text{-ideals.}$$

Finally, $(\frac{\lambda}{\gamma^2})\mathcal{O}_K$ is an S-ideal, which implies that $u := \frac{\lambda}{\gamma^2}$ is an S-unit. Now, by dividing $\mu + 4 = \lambda$ by u, we get:

$$\alpha + \beta = \gamma^2 \text{ where } \alpha := \frac{\mu}{u} \in \mathcal{O}^*_{S_K} \text{ and } \beta := \frac{4}{u} \in \mathcal{O}^*_{S_K} \tag{13}$$

Now, suppose that there is some $\tilde{\mathfrak{P}} \in S_K$ that satisfies $|v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta})| \leq 6v_{\tilde{\mathfrak{P}}}(2)$. We will show that this leads to a contradiction with 3.7 (iv) (i.e. $v_{\tilde{\mathfrak{P}}}(j_{E'}) < 0$), and hence conclude the proof.
By using (13) we can rewrite our assumption in terms of the valuation of μ: $-4v_{\tilde{\mathfrak{P}}}(2) \leq v_{\tilde{\mathfrak{P}}}(\mu) \leq 8v_{\tilde{\mathfrak{P}}}(2)$. Note that $j_{E'} = 2^8(\mu + 1)^3\mu^{-1}$, hence $v_{\tilde{\mathfrak{P}}}(j_{E'}) = 8v_{\tilde{\mathfrak{P}}}(2) + 3v_{\tilde{\mathfrak{P}}}(\mu + 1) - v_{\tilde{\mathfrak{P}}}(\mu)$. There are three cases according to the valuation of $\tilde{\mathfrak{P}}$ at μ:
Case (1): Suppose $v_{\tilde{\mathfrak{P}}}(\mu) = 0$. This implies that $v_{\tilde{\mathfrak{P}}}(\mu + 1) \geq 0$, thus $v_{\tilde{\mathfrak{P}}}(j_{E'}) \geq 0$, a contradiction.

Case (2): Suppose $v_{\tilde{\mathfrak{P}}}(\mu) > 0$. This implies $v_{\tilde{\mathfrak{P}}}(\mu+1) = 0$, thus, by using $v_{\tilde{\mathfrak{P}}}(\mu) \leq 8v_{\tilde{\mathfrak{P}}}(2)$ we get again $v_{\tilde{\mathfrak{P}}}(j_{E'}) \geq 0$.
Case (3): Finally, suppose $v_{\tilde{\mathfrak{P}}}(\mu) < 0$. This implies $v_{\tilde{\mathfrak{P}}}(\mu+1) = v_{\tilde{\mathfrak{P}}}(\mu)$, thus, by using $-4v_{\tilde{\mathfrak{P}}}(2) \leq v_{\tilde{\mathfrak{P}}}(\mu)$, we get one last time $v_{\tilde{\mathfrak{P}}}(j_{E'}) \geq 0$.
All three cases lead to contradictions and hence we conclude the proof. □

4 Proof of Main Theorem for signature $(p, p, 3)$

This section is dedicated to proving Theorem 1.7. Let K be a totally real field. Recall the sets:

$$S_K = \{\mathfrak{P} \ : \mathfrak{P} \text{ is a prime of } K \text{ above } 3\}$$

$U_{K,\mathfrak{P}} = \{(a,b,c) \in \mathcal{O}_K^3 : a^p + b^p = c^3 \text{ with } \mathfrak{P}|b\}$, where $\mathfrak{P} \in S_K$ is a fixed prime.

4.1 Frey Curve

For a non-trivial, primitive solution (a,b,c) of $a^p + b^p = c^3$ we associate the following Frey elliptic curve defined over K:

$$E : Y^2 + 3cXY + a^pY = X^3 \tag{14}$$

We use [30] (III.1) to compute the arithmetic invariants:

$$\Delta_E = 3^3(a^3b)^p,\ c_4 = 3^2c^3(9b^p + a^p)^3 \text{ and } j_E = 3^3\frac{c^3(9b^p+a^p)^3}{(a^3b)^p}.$$

Lemma 4.1. *Let (a,b,c) be the non-trivial, primitive solution to the equation $a^p + b^p = c^3$. Let E be the associated Frey curve (14) with conductor $\mathcal{N}_E$. Then, for all primes $\mathfrak{q} \notin S_K$, the model E is minimal, semistable and satisfies $p|v_{\mathfrak{q}}(\Delta_E)$. Moreover*

$$\mathcal{N}_E = \prod_{\mathfrak{P}\in S_K} \mathfrak{P}^{r_{\mathfrak{P}}} \prod_{\substack{\mathfrak{q}|ab \\ \mathfrak{q}\notin S_K}} \mathfrak{q},\ \mathcal{N}_p = \prod_{\mathfrak{P}\in S_K} \mathfrak{P}^{r'_{\mathfrak{P}}} \tag{15}$$

where $0 \leq r'_{\mathfrak{P}} \leq r_{\mathfrak{P}} \leq 2 + 3v_{\mathfrak{P}}(3)$.

Proof. Let $\mathfrak{q}$ be an a prime of K which does not divide 3. The invariants of the model E are $\Delta_E = 3^3(a^3b)^p$ and $c_4 = 3^2c^3(9b^p + a^p)^3$ Suppose that $\mathfrak{q}$ divides Δ_E, so $\mathfrak{q}|ab$. Since a, b and c are pairwise coprime, $\mathfrak{q}$ divides exactly one of a and b, but not c. Therefore, $\mathfrak{q}$ does not divide c_4. In particular, $v_{\mathfrak{q}}(c_4) < 4$ and as the coefficients of E are in $\mathcal{O}_K$ we can use [30] VII.1 Remark 1.1. to deduce that the model is minimal at q and [30] VII.5. Proposition 5.1. to deduce that E has multiplicative reduction at $\mathfrak{q}$ as $v_{\mathfrak{q}}(\Delta_E) > 0$ and $v_{\mathfrak{q}}(c_4) = 0$. Hence $p|v_{\mathfrak{q}}(\Delta_E) = v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$. On the other hand, if $\mathfrak{P} \in S_K$, a

prime which divides 3, we have $r_{\mathfrak{P}} = v_{\mathfrak{P}}(\mathcal{N}_E) \leq 2 + 3v_{\mathfrak{P}}(3)$ by [31] Theorem IV.10.4. The definition of $\mathcal{N}_E$ gives the desired form in (15). Then, use (10) to get $\mathcal{N}_p$ and observe that $r'_{\mathfrak{P}} = r_{\mathfrak{P}}$ unless E has multiplicative reduction at $\mathfrak{P}$ and $p|v_{\mathfrak{P}}(\Delta_{\mathfrak{P}})$ in which case $r_{\mathfrak{P}} = 1$ and $r'_{\mathfrak{P}} = 0$. □

Lemma 4.2. *Let K be a totally real field. There is some constant A_K depending only on K, such that for any non-trivial, primitive solution (a, b, c) of $a^p + b^p = c^3$ the Frey curve given by (14) is modular.*

Proof. The proof uses the same idea as the proof of Lemma 3.2, but note that here, by taking $\lambda := b^p/a^p$ we will get

$$j(\lambda) = 3^3(\lambda + 1)(9\lambda + 1)^3\lambda^{-1}$$

so each equation $j(\lambda) = j_i$ will have at most four solutions. From here the argument works exactly as before. □

4.2 Images of Inertia

Lemma 4.3. *Let $\mathfrak{q} \nmid 3$ and let (a, b, c) be a non-trivial, primitive solution to the equation $a^p + b^p = c^3$ with the prime exponent $p \geq 5$, such that $\mathfrak{q} \nmid p$. Let E be the Frey curve in (14). Then $p \nmid \#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$.*

Proof. The proof follow exactly like in Lemma 3.5 by replacing all of the "2" with "3". □

Lemma 4.4. *Let $\mathfrak{P} \in S_K$ and $(a, b, c) \in U_{K,\mathfrak{P}}$ with prime exponent $p > 3v_{\mathfrak{P}}(3)$. Let E be the Frey curve in (14) with j-invariant j_E. Then E has potentially multiplicative reduction at $\mathfrak{P}$ and $p|\#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$.*

Proof. The proof follows exactly like the proof of Lemma 3.6 by replacing all of the "$6v_{\mathfrak{P}}(2)$" with "$3v_{\mathfrak{P}}(3)$". □

4.3 Level Lowering and Eichler Shimura

As in the previous section, the crucial level lowering theorem reads as follows:

Theorem 4.5. *Let K be a totally real number field and assume it has a distinguished prime $\tilde{\mathfrak{P}} \in S_K$. Then there is a constant B_K depending only on K such that the following hold. Let $(a, b, c) \in U_{K,\tilde{\mathfrak{P}}}$ non-trivial, primitive with prime exponent $p > B_K$. Write E for the Frey curve (14). Then, there is an elliptic curve E' over K such that:*

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

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

(iii) E' has a K-rational point of order 3;

(iv) E' has multiplicative reduction at $\tilde{\mathfrak{P}}$ ($v_{\tilde{\mathfrak{P}}}(j_{E'}) < 0$ where $j_{E'}$ is the j-invariant of E').

Proof. The proof follows exactly like the proof of Theorem 3.7 by replacing 2 by 3. □

4.4 Proof of the Main Theorem

Proof. So far, we have shown that for a primitive, non-trivial solution $(a, b, c) \in U_{K,\tilde{\mathfrak{P}}}$ with a prime exponent p we associate the Frey elliptic curve in (14). By Theorem 4.5 for $p > B_K$ we can find an elliptic curve E' which is related to E by $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$ and has a K-rational point of order 3. Hence by Theorem 2.3 (ii) we get a model:

$$E' : Y^2 + c'XY + d'Y = X^3$$

with arithmetic invariants $\Delta_{E'} = d'^3(c'^3 - 27d')$ and $j_{E'} = \frac{c'^3(c'^3-24d')^3}{d'^3(c'^3-27d')}$. Moreover, by Theorem 3.7 (i), we know that E' has good reduction outside S_K which implies that $v_{\mathfrak{q}}(j_{E'}) \geq 0$ for $\mathfrak{q} \notin S_K$. Therefore, $j_{E'} \in \mathcal{O}_{S_K}$. Consider $\lambda := \frac{c'^3}{d'}$ and $\mu := \lambda - 27 = \frac{c'^3-27d'}{d'}$. Next, we need to show that λ can be written as $\lambda = u\gamma^3$, where u is an S_K-unit.
By Lemma 2.5 (ii) applied to E' we get that

$$(\lambda)\mathcal{O}_K = I^3 J \text{ where } J \text{ is an } S\text{-ideal.}$$

Thus $[I]^3 = [J]$ as elements of the class group $\mathrm{Cl}(K)$ and $[J] \in \langle[\mathfrak{P}]\rangle_{\mathfrak{P}\in S_K}$. This implies that $[I] \in Cl_{S_K}(K)[3]$ and by our assumption on K that $Cl_{S_K}(K)[3]$ is trivial, we get that $[I] \in \langle[\mathfrak{P}]\rangle_{\mathfrak{P}\in S_K}$, i.e. $I := \gamma\tilde{I}$, where $\tilde{I}$ is an S-ideal and $\gamma \in \mathcal{O}_K$. Consequently,

$$(\lambda)\mathcal{O}_K = (\gamma)^3\tilde{I}^3 J \text{ where both } \tilde{I} \text{ and } J \text{ are } S\text{-ideals.}$$

Finally, $(\frac{\lambda}{\gamma^3})\mathcal{O}_K$ is an S-ideal, which implies that $u := \frac{\lambda}{\gamma^3}$ is an S-unit. Now, by dividing $\mu + 27 = \lambda$ by u, we get:

$$\alpha + \beta = \gamma^3 \text{ where } \alpha := \frac{\mu}{u} \in \mathcal{O}^*_{S_K} \text{ and } \beta := \frac{27}{u} \in \mathcal{O}^*_{S_K} \tag{16}$$

Now, suppose that there is some distinguished $\tilde{\mathfrak{P}} \in S_K$ that satisfies $|v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta})| \leq 3v_{\tilde{\mathfrak{P}}}(3)$. We will show that this leads to a contradiction with 3.7 (iv) (i.e. $v_{\tilde{\mathfrak{P}}}(j_{E'}) < 0$), and hence conclude the proof.
By using (16) we can rewrite our assumption in terms of the valuation of μ: $0 \leq v_{\tilde{\mathfrak{P}}}(\mu) \leq 6v_{\tilde{\mathfrak{P}}}(3)$. Note that $j_{E'} = (\mu + 27)(\mu + 3)^3\mu^{-1}$, hence $v_{\tilde{\mathfrak{P}}}(j_{E'}) = v_{\mathfrak{P}}(\mu+27) + 3v_{\mathfrak{P}}(\mu+3) - v_{\mathfrak{P}}(\mu)$. There are three cases according to the valuation of $\tilde{\mathfrak{P}}$ at μ:
Case (1): Suppose $0 \leq v_{\tilde{\mathfrak{P}}}(\mu) \leq v_{\tilde{\mathfrak{P}}}(3)$. This implies that $v_{\tilde{\mathfrak{P}}}(\mu + 27) =$

$v_{\tilde{\mathfrak{P}}}(\mu)$ and $v_{\tilde{\mathfrak{P}}}(\mu+3) \geq v_{\tilde{\mathfrak{P}}}(\mu)$, thus $v_{\tilde{\mathfrak{P}}}(j_{E'}) \geq 0$.
Case (2): Suppose $v_{\tilde{\mathfrak{P}}}(3) < v_{\tilde{\mathfrak{P}}}(\mu) \leq 3v_{\tilde{\mathfrak{P}}}(3)$. This implies that $v_{\tilde{\mathfrak{P}}}(\mu+27) \geq v_{\tilde{\mathfrak{P}}}(\mu)$ and $v_{\tilde{\mathfrak{P}}}(\mu+3) = v_{\tilde{\mathfrak{P}}}(3)$, thus we get again $v_{\tilde{\mathfrak{P}}}(j_{E'}) \geq 0$.
Case (3): Suppose $3v_{\tilde{\mathfrak{P}}}(3) < v_{\tilde{\mathfrak{P}}}(\mu) \leq 6v_{\tilde{\mathfrak{P}}}(3)$. This implies that $v_{\tilde{\mathfrak{P}}}(\mu+27) = 3v_{\tilde{\mathfrak{P}}}(3)$ and $v_{\tilde{\mathfrak{P}}}(\mu+3) = v_{\tilde{\mathfrak{P}}}(3)$, thus we get one last time $v_{\tilde{\mathfrak{P}}}(j_{E'}) \geq 0$.
All three cases lead to contradictions and hence we conclude the proof. □

5 S-unit equations and computability

Finally, we will describe how to algorithmically check the hypothesises in our two main theorems 1.5 and 1.7 by studying how to compute solutions of certain (linear) *S-unit equations* over the totally real number field K, i.e. equations of the form:

$$ax + by = 1 \text{ where } a, b \in K^* \text{ with solutions } x, y \in \mathcal{O}_S^*.$$

Throughout this section S denotes a finite set of prime ideals in $\mathcal{O}_K$.
More generally, S-unit equations play a crucial role in Number Theory. They have many fruitful applications: in Algebraic Number Theory, Transcendental Number Theory, and moreover, in irreducible polynomials and arithmetic graphs, finitely generated groups, and beyond. See Evertse's [11] for a comprehensive survey about this.
They have been of particular interest in the study of certain problems about elliptic curves. Siegel's famous result about the finiteness of S-integral points on affine curves C/K of genus at least one reduces to solving several linear S-units equations of the form $ax + by = 1$. See [30] (IX.4.) for more details. Recently, they were used to parametrise different families of elliptic curves, in particular this was a crucial step in both [14] and [21] (and consequently, in this project) when finding the lever lowered elliptic curves with full 2-torsion and one 2-torison point respectively. Another application of a similar flavour can be found in [20] where Koutsianas uses S-unit equations to find the j-invariants of all elliptic curves of good reduction outside S.
The reason why people turned their attention to S-unit equations is because they have a finite number of solutions, effectively computable, which thanks to the increased computer power available, turned out to be a powerful tool in modern Number Theory.
The following result is vital for our discussion:

Theorem 5.1. *Let K be a number field and $S \subset \mathcal{O}_K$ a finite set of prime ideals, and let $a, b \in K^*$. Then, the equation*

$$ax + by = 1$$

has only finitely many solutions in $\mathcal{O}_S^*$.

Proof. For an ineffective proof of this see [30] (IX.4.) or [27]. □

Remark 5.2. More recently, methods of effectively computing solutions to S-unit equations became available, pioneered by De Weger's famous thesis [36] for the special case $K = \mathbb{Q}$. His method of lattice approximation reduction algorithms was later generalized for all number fields by others, see for example Smart's [32].
An S-unit solver for $a = b = 1$ has been implemented in the free open-source mathematics software by A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, D. Roe, C. Vincent, M. West in [1].

In the two main results of this project, we would like to compute the solutions of two non-linear S-unit equations. Namely, in Theorem 1.5 we work with $\alpha+\beta=\gamma^2$, and similarly, in Theorem 1.7 with $\alpha+\beta=\gamma^3$, where $\alpha, \beta \in \mathcal{O}_{S_K}^*,\ \gamma \in \mathcal{O}_{S_K}$ in both cases. The next result shows that these can be reduced to solving a finite set of linear $S-$unit equations.

Theorem 5.3. *Let K be a totally real number field and $S \subset \mathcal{O}_K$ a finite set of prime ideals and consider the equation:*

$$\alpha + \beta = \gamma^i,\ \alpha, \beta \in \mathcal{O}_S^*,\ \gamma \in \mathcal{O}_S.$$

(i) If $i = 2$, the equation has a finite number of solutions with $\gcd(\alpha, \beta)$ *square-free;*

(ii) If $i = 3$ the above equation has a finite number of solutions with $\gcd(\alpha, \beta)$ *cube-free.*

In both cases, the solutions are effectively computable.

Proof. (i) Let $i = 2$. Then, we can write $\alpha + \beta = \gamma^2$ as:

$$(\gamma - \sqrt{\beta})(\gamma + \sqrt{\beta}) = \alpha \text{ over } K(\sqrt{\beta}).$$

Denote $x := \gamma - \sqrt{\beta}$, $y := \gamma + \sqrt{\beta}$, $L := K(\sqrt{\beta})$ and $S' := \{\mathfrak{P}_L \text{ prime of } \mathcal{O}_L : \mathfrak{P}_L | \mathfrak{P}_K \in S\}$. Note that S' is a finite set as S is finite and $[L : K] \leq 2$. Working over L, we get $x, y \in \mathcal{O}_{S'}^*$. This can be seen by simply considering the valuation of the product $xy = \alpha \in \mathcal{O}_S^*$ at primes of L outside the set S'.
Note that $x - y = -2\sqrt{\beta}$ (17). Letting:

$$X := \frac{x}{2\sqrt{\beta}},\ Y := \frac{-y}{2\sqrt{\beta}} \text{ we get X+Y=1. (18)}$$

The desired solutions can be recovered as $\alpha = -4\beta XY$, $\beta = \beta(X + Y)^2 = \beta$. So the square-free condition reduces to β is square-free, implying $\beta \in \mathcal{O}_S^*/(\mathcal{O}_S^*)^2$. By Remark 2.1 we know that $\mathcal{O}_S^*$ is finitely

generated, hence the quotient $\mathcal{O}_S^*/(\mathcal{O}_S^*)^2$ is finite and computable. ($\star$)
By Theorem 5 (with $a = b = 1$), (18) has a finite number of solutions (X, Y) and by Remark 5.2 the solutions are effectively computable.($\star\star$)
By ($\star$) and ($\star\star$) each L gives a finite set of solutions $(\alpha, \beta) \in \mathcal{O}_S^* \times \mathcal{O}_S^*$.

Now, let's prove it is enough to consider only finitely many fields $L = K(\sqrt{\beta})$ for our purpose (of finding α and β). This follows from the fact that we only get different extensions when $\beta \in \mathcal{O}_S^*/(\mathcal{O}_S^*)^2$, which we just proved to be a finite set.

(ii) Let $i = 3$. We can write $\alpha + \beta = \gamma^3$ as:

$$(\gamma - \sqrt[3]{\beta})(\gamma - \omega\sqrt[3]{\beta})(\gamma - \omega^2\sqrt[3]{\beta}) = \alpha \text{ over } K(\omega, \sqrt[3]{\beta})$$

where $\omega := \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$ if $\beta \neq -1$.

Denote $x := \gamma - \sqrt[3]{\beta}$, $y := \gamma - \omega\sqrt[3]{\beta}$, $z := \gamma - \omega^2\sqrt[3]{\beta}$, $L := K(\omega, \sqrt[3]{\beta})$ and $S' := \{\mathfrak{P}_L \text{ prime of } \mathcal{O}_L : \mathfrak{P}_L | \mathfrak{P}_K \in S\}$. We make the quick note that if $\beta = -1$ we take $x := \gamma + 1$, $y := \gamma + \omega$, $z := \gamma + \omega^2$, $L := K(\omega)$. The same arguments as above give S' finite and $x, y, z \in \mathcal{O}_{S'}^*$.
Note that

$$\begin{cases} x - y = (\omega - 1)\sqrt[3]{\beta} \\ y - z = (\omega^2 - \omega)\sqrt[3]{\beta} \end{cases} \tag{19}$$

By letting

$$X := \frac{1}{(\omega - 1)\sqrt[3]{\beta}}x,\ Y := \frac{-1}{(\omega - 1)\sqrt[3]{\beta}}y,\ Z := \frac{-1}{(\omega^2 - \omega)\sqrt[3]{\beta}}z$$

we get:

$$\begin{cases} X + Y = 1 \\ \frac{-1}{\omega}Y + Z = 1 \end{cases} \tag{20}$$

The desired α can be recovered as $\alpha = -3(\omega + 2)XYZ\beta$. So the cube-free condition reduces to β is cube-free, implying $\beta \in \mathcal{O}_S^*/(\mathcal{O}_S^*)^3$. By Remark 2.1 we know that $\mathcal{O}_S^*$ is finitely generated, hence the quotient $\mathcal{O}_S^*/(\mathcal{O}_S^*)^3$ is finite and computable. (†)
By Theorem 5 (with $a = b = 1$ applied to 20), there are finitely many pairs (X, Y) and $Z = 1 + \frac{1}{\omega}Y$ by Remark 5.2 the solutions are effectively computable.(††)
By (†) and (††) each L gives a finite set of solutions $(\alpha, \beta) \in \mathcal{O}_S^* \times \mathcal{O}_S^*$.

Now, let's prove it is enough to consider only finitely many fields $L := K(\omega, \sqrt[3]{\beta})$ for our purpose (of finding α and β). This follows from the fact that we only get different extensions when $\beta \in \mathcal{O}_S^*/(\mathcal{O}_S^*)^3$, which we just proved to be a finite set.

□

Remark 5.4. On a computational note, we can restrict the search of our solutions in the following way:

(i) In (17) we are only looking for the solutions $(x, y) \in \mathcal{O}_{S'}^* \times \mathcal{O}_{S'}^*$ such that $xy \in \mathcal{O}_S^*$ and $\sigma(x) = y$, where σ is the generator of $\mathrm{Gal}(L/K) = \{\mathrm{id}, \sigma\}$. In particular, $\sigma(X) = Y$ which we will use in our computations.

(ii) Similarly, in (19) we only need to search for $(x, y, z) \in \mathcal{O}_{S'}^* \times \mathcal{O}_{S'}^* \times \mathcal{O}_{S'}^*$ such that $xyz \in \mathcal{O}_S^*$ and $\tau(x) = y$, $\tau^2(x) = z$, where τ is the element of $\mathrm{Gal}(L/K(\omega))$ such that $\tau(\sqrt[3]{\beta}) = \omega\sqrt[3]{\beta}$.

Corollary 5.5. *Let K be a totally real number field and $S \subset \mathcal{O}_K$ a finite set of prime ideals and consider the equation:*

$$\alpha + \beta = \gamma^i,\ \alpha, \beta \in \mathcal{O}_S^*,\ \gamma \in \mathcal{O}_S$$

with $i \in \{1, 2\}$.
Then α/β belongs to a finite computable set.

Proof. We give an effective method to compute α/β by following the steps in the proof of Theorem 5.3. Note that as we are only interested in the ratio α/β we can assume $\gcd(\alpha, \beta) = 1$.

(i) If $i = 2$ we get $\frac{\alpha}{\beta} = -4XY$ where $X + Y = 1$ is an S'-unit as described in (18). So it is enough to compute a finite number of S'-unit equations (one for each L) to get $\frac{\alpha}{\beta}$. We have algorithms to solve each of these S'-unit equations by Remark 5.2.

(ii) If $i = 3$ we get $\frac{\alpha}{\beta} = -3(\omega + 2)XYZ = -3(\omega + 2)XY(1 + \frac{1}{\omega}Y)$ where $X + Y = 1$ is an S'-unit and $Z = 1 + \frac{1}{\omega}Y$ as described in (20). So it is enough to compute a finite number of S'-unit equations (one for each L) to get $\frac{\alpha}{\beta}$. We have algorithms to solve each of these S'-unit equations by Remark 5.2.

□

6 Examples for signature $(p, p, 2)$

In this section, we give a few examples of totally real fields K on which the asymptotic Fermat Last Theorem holds for $a^p + b^p = c^2$. We present three examples: $K_1 = \mathbb{Q}(\sqrt{2})$, $K_2 = \mathbb{Q}(\sqrt{26})$, $K_3 = \mathbb{Q}(\sqrt{35})$. The field K_1 has narrow class number one and it satisfies the conditions in Theorem 1.3 (proved in [21]). The fields K_1 and K_2 have class number 2, so we can no longer use Theorem 1.3. However $\mathrm{CL}_{S_K}(K)[2]$ is trivial, so we use our Main

Theorem for $(p,p,2)$ (Theorem 1.5) to prove that the asymptotic Fermat Last Theorem holds for $a^p+b^p=c^2$ over K_1 and K_2.
We are in the set-up of Section 3, so recall the sets:

$$S_K=\{\mathfrak{P}\ :\mathfrak{P}\text{ is a prime of }K\text{ above }2\},\quad T_K=\{\mathfrak{P}\in S_K : f(\mathfrak{P}/2)=1\}$$

$$W_K=\{(a,b,c)\in\mathcal{O}_K^3 : a^p+b^p=c^2 \text{ with } \mathfrak{P}|b \text{ for every } \mathfrak{P}\in T_K\}$$

$U_{K,\mathfrak{P}}=\{(a,b,c)\in\mathcal{O}_K^3 : a^p+b^p=c^2 \text{ with } \mathfrak{P}|b\}$, where $\mathfrak{P}\in S_K$ is a fixed prime.

Naturally, $S_L=\{\mathfrak{P}\ :\mathfrak{P}\text{ is a prime of }L\text{ above }2\}$.

Corollary 6.1. *Let $K_1=\mathbb{Q}(\sqrt{2})$ and $\tilde{\mathfrak{P}}=(\sqrt{2})\mathcal{O}_{K_1}$. Then $a^p+b^p=c^2$ does not have any non-trivial, primitive solution (a,b,c) in K_1 such that $\tilde{\mathfrak{P}}|b$ whenever $p\geq B_{K_1}$ where B_{K_1} is a constant that depends only on K_1.*

Proof. As $h_K^+=1$ (where h_K^+ represents the narrow class number), we want to prove the conditions in Theorem 1.3 are satisfied. In [21], Section 6, Işik, Kara and Ozman compute the solutions of the S-unit equation $\lambda+\mu=1$ over K_1 and over L where $L=K_1(\sqrt{a})$ for $a\in K(S_K,2)$. The list of such L is below:

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

After computing the above-mentioned solutions, they check that the criteria in (A) and (B) of Theorem 1.3 are satisfied, and hence prove the corollary. Moreover, they compute (a non-optimal) bound $B_{K_1}=282430599364$. See their paper [21] Section 6 for the details. □

Corollary 6.2. *Let $K_2=\mathbb{Q}(\sqrt{26})$ and $\tilde{\mathfrak{P}}=(2,\sqrt{26})\mathcal{O}_{K_2}$. Then $a^p+b^p=c^2$ does not have any non-trivial, primitive solution (a,b,c) in K_2 such that $\tilde{\mathfrak{P}}|b$ whenever $p\geq B_{K_2}$ where B_{K_2} is a constant that depends only on K_2.*

Proof. We prove that we are in the set-up of Theorem 1.5, more precisely we want to show that for every solution (α,β) to the S_{K_2}-unit equation $\alpha+\beta=\gamma^2$ we get that $|v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta})|\leq 6v_{\tilde{\mathfrak{P}}}(2)$.

By the proof of Corollary 5.5 (i) applied on $K_2 = \mathbb{Q}(\sqrt{26})$ and $S = S_{K_2}$, we get

$$v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta}) = v_{\tilde{\mathfrak{P}}}(-4XY) \tag{21}$$

where $X + Y = 1$ is an S_L-unit equation on $L = K_2(\sqrt{\beta})$ (note that S' becomes S_L). By Theorem 5.3 (i) we only need to consider $\beta \in \mathcal{O}^*_{S_{K_2}}/(\mathcal{O}^*_{S_{K_2}})^2$ for our purpose. Hence we end up with the following cases:

- $L_0 = K_2 = \mathbb{Q}(a_0)$ where a_0 is a root of $x^2 - 26$
- $L_1 = \mathbb{Q}(a_1)$ where a_1 is a root of $x^4 - 50x^2 + 729$
- $L_2 = \mathbb{Q}(a_2)$ where a_2 is a root of $x^4 - 10x^2 - 1$
- $L_3 = \mathbb{Q}(a_3)$ where a_3 is a root of $x^4 - 56x^2 + 576$
- $L_4 = \mathbb{Q}(a_4)$ where a_4 is a root of $x^4 + 10x^2 - 1$
- $L_5 = \mathbb{Q}(a_5)$ where a_5 is a root of $x^4 - 48x^2 + 784$
- $L_6 = \mathbb{Q}(a_6)$ where a_6 is a root of $x^4 - 20x^2 - 4$
- $L_7 = \mathbb{Q}(a_7)$ where a_7 is a root of $x^4 + 20x^2 - 4$

We used the S-unit solver in Sage by A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, D. Roe, C. Vincent, M. West in [1] to compute solutions to the S_L-unit equation $X + Y = 1$ over $L_0, L_1, L_2, L_4, L_5, L_6, L_7$. See Appendix A. By Remark 5.4, it is enough to consider $X+Y = 1$ with $\sigma(X) = Y$ where σ is the generator of $\mathrm{Gal}(L_i/K_2) = \{\mathrm{id}, \sigma\}, 1 \leq i \leq 7$. This is particularly useful in the case of L_3 and L_6.
We check using Sage that for each of these solutions

$$v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta}) \overset{(21)}{=} v_{\tilde{\mathfrak{P}}}(-4XY) \leq 6v_{\tilde{\mathfrak{P}}}(2).$$

Therefore, we are only left with the case L_3. Here, we came across some computational limitations of the above-mentioned S-unit solver, so we will treat this case by studying how 2 lifts in L_3.
The extension L_3 is given by $L_3 = K_2(\sqrt{2})$. The prime decomposition of 2 is as follows:

$$\begin{cases} (2)\mathcal{O}_{K_2} = \tilde{\mathfrak{P}}^2 \text{ where } \tilde{\mathfrak{P}} = (2, \sqrt{26})\mathcal{O}_{K_2} \\ (2)\mathcal{O}_{L_3} = \mathfrak{P}_L^2 \text{ where } \mathfrak{P}_L = (\sqrt{2})\mathcal{O}_{L_3} \end{cases}$$

In particular, $S_{K_2} = \{\tilde{\mathfrak{P}}\}$ and $S_{L_3} = \{\mathfrak{P}_L\}$. We examine the S_{L_3}-unit solutions of $X + Y = 1$ where we require $X = \sigma(Y)$ for σ the generator of $\mathrm{Gal}(L_3/K_2) = \{\mathrm{id}, \sigma\}$. Note that $\sigma(\mathfrak{P}_L) = \mathfrak{P}_L$. Therefore $v_{\mathfrak{P}_L}(X) = v_{\mathfrak{P}_L}(Y)$.

Suppose $v_{\mathfrak{P}_L}(X) = v_{\mathfrak{P}_L}(Y) > 0$, then $\mathfrak{P}_L|1$, a contradiction. Hence, we have $v_{\mathfrak{P}_L}(X) = v_{\mathfrak{P}_L}(Y) := s \leq 0$, giving $XY = 2^s t$, where t is a unit. Finally

$$v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta}) \overset{(21)}{=} v_{\tilde{\mathfrak{P}}}(-4XY) = (2+s)v_{\tilde{\mathfrak{P}}}(2) \leq 6v_{\tilde{\mathfrak{P}}}(2).$$

By symmetry of α and β we get $v_{\tilde{\mathfrak{P}}}(\frac{\beta}{\alpha}) = -v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta}) \leq 6v_{\tilde{\mathfrak{P}}}(2)$ and hence we can conclude the proof by Theorem 1.5 as promised.

□

Corollary 6.3. *Let $K_3 = \mathbb{Q}(\sqrt{35})$ and $\tilde{\mathfrak{P}} = (2, \sqrt{35}+1)\mathcal{O}_{K_3}$. Then $a^p + b^p = c^2$ does not have any non-trivial, primitive solution (a, b, c) in K_3 such that $\tilde{\mathfrak{P}}|b$ whenever $p \geq B_{K_3}$ where B_{K_3} is a constant that depends only on K_3.*

Proof. As in the previous example, we prove that we are in the set-up of Theorem 1.5, more precisely we want to show that for every solution (α, β) to the S_{K_3}-unit equation $\alpha + \beta = \gamma^2$ we get that $|v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta})| \leq 6v_{\tilde{\mathfrak{P}}}(2)$.
By the proof of Corollary 5.5 (i) applied on $K_3 = \mathbb{Q}(\sqrt{35})$ and $S = S_{K_3}$, we get

$$v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta}) = v_{\tilde{\mathfrak{P}}}(-4XY) \tag{22}$$

where $X + Y = 1$ is an S_L-unit equation of $L = K_2(\sqrt{\beta})$ (note that S' becomes S_L). By Theorem 5.3 (i) we only need to consider $\beta \in \mathcal{O}^*_{S_{K_3}}/(\mathcal{O}^*_{S_{K_3}})^2$ for our purpose. Hence we end up with the following cases:

- $L_0 = K_3 = \mathbb{Q}(a_0)$ where a_0 is a root of $x^2 - 35$
- $L_1 = \mathbb{Q}(a_1)$ where a_1 is a root of $x^4 - 68x^2 + 1296$
- $L_2 = \mathbb{Q}(a_2)$ where a_2 is a root of $x^4 - 12x^2 + 1$
- $L_3 = \mathbb{Q}(a_3)$ where a_3 is a root of $x^4 - 74x^2 + 1089$
- $L_4 = \mathbb{Q}(a_4)$ where a_4 is a root of $x^4 + 12x^2 + 1$
- $L_5 = \mathbb{Q}(a_5)$ where a_5 is a root of $x^4 - 66x^2 + 1369$
- $L_6 = \mathbb{Q}(a_6)$ where a_6 is a root of $x^4 - 24x^2 + 4$
- $L_7 = \mathbb{Q}(a_7)$ where a_7 is a root of $x^4 + 24x^2 + 4$

As before, we used the S-unit solver in Sage by A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, D. Roe, C. Vincent, M. West in [1] to compute solutions to the S_L-unit equation $X + Y = 1$ over L_0, L_1, L_4, L_5, L_7.
We came across some computational limitations of this S-unit solver for the field extensions L_2, L_3 and L_6. However, Benjamin Matschke kindly offered to compute the S-unit equations in these cases, using his independent S-unit solver which can be found at `https://github.com/bmatschke/`

`s-unit-equations`.
All the above-mentioned solutions can be found in Appendix B. We check using Sage that for each of these solutions

$$v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta}) \overset{(21)}{=} v_{\tilde{\mathfrak{P}}}(-4XY) \leq 6v_{\tilde{\mathfrak{P}}}(2).$$

By symmetry of α and β we get $v_{\tilde{\mathfrak{P}}}(\frac{\beta}{\alpha}) = -v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta}) \leq 6v_{\tilde{\mathfrak{P}}}(2)$ and hence we can conclude the proof by Theorem 1.5 as promised. □

Remark 6.4. The field extensions L that we need to inspect as part of solving $\alpha+\beta = \gamma^2$ in Theorem 1.5 are the same as the ones in the assumptions of Theorem 1.3. This is easy to see from the Kummer exact sequence in (3) with $n = 2$.

Remark 6.5. The choice of the quadratic fields $K_2 = \mathbb{Q}(\sqrt{26})$ and $K_3 = \mathbb{Q}(\sqrt{35})$ might seem aleatory, but the reason why we chose them this way is because the S-unit solver seem to perform better on these number fields.

7 Examples for signature $(p, p, 3)$

We are in the set-up of Section 4, so recall the sets:

$$S_K = \{\mathfrak{P} \ : \mathfrak{P} \text{ is a prime of } K \text{ above } 3\}$$

$U_{K,\mathfrak{P}} = \{(a, b, c) \in \mathcal{O}_K^3 : a^p+b^p = c^3 \text{ with } \mathfrak{P}|b\}$, where $\mathfrak{P} \in S_K$ is a fixed prime.

Corollary 7.1. *Suppose $K = \mathbb{Q}(\sqrt{d})$ with d a positive square-free integer and $d \equiv 2 \mod 3$. Then 3 is inert in K. Take $\tilde{\mathfrak{P}} = (3)\mathcal{O}_K$. Assume moreover that $Cl_{S_K}(K)[3]$ is trivial. Then $a^p + b^p = c^3$ does not have any non-trivial, primitive solution (a, b, c) in K such that $3|b$ whenever $p \geq B_K$ where B_K is a constant that depends only on K.*

Proof. We prove that we are in the set-up of Theorem 1.7, more precisely we want to show that for every solution (α, β) to the S_K-unit equation $\alpha+\beta = \gamma^3$ we get that $|v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta})| \leq 3v_{\tilde{\mathfrak{P}}}(3)$.
We will make use of the notations in Theorem 5.3 (ii). Recall that $\alpha+\beta = \gamma^3$ leads to an equation

$$(\gamma - \sqrt[3]{\beta})(\gamma - \omega\sqrt[3]{\beta})(\gamma - \omega^2\sqrt[3]{\beta}) = \alpha \text{ over } K(\omega, \sqrt[3]{\beta})$$

We denoted

$$\begin{cases} x := \gamma - \sqrt[3]{\beta}, y := \gamma - \omega\sqrt[3]{\beta}, z := \gamma - \omega^2\sqrt[3]{\beta}, L := K(\omega, \sqrt[3]{\beta}), \text{ if } \beta \neq -1 \\ x := \gamma + 1, y := \gamma + \omega, z := \gamma + \omega^2, L := K(\omega), \text{ if } \beta = -1. \end{cases} \tag{23}$$

Now, we slightly deviate from the proof of Theorem 5.3. As 3 is inert in K, it follows that $\tilde{\mathfrak{P}} = (3)\mathcal{O}_K$ and $S_K = \{(3)\mathcal{O}_K\}$. Thus, $\mathcal{O}^*_{S_K} = \{3^k \text{ for } k \text{ integer}\}$.
Case (1): If $\beta \neq \pm 1$ and $\beta \in \mathcal{O}^*_{S_K} \setminus (\mathcal{O}^*_{S_K})^3$ we have that $[L : K] = 6$ by (23). Standard algebraic number theory gives $\mathcal{O}_L = \mathcal{O}_K(\omega, \sqrt[3]{\beta})$. So, by Dedekind Theorem, it follows that

$$(3)\mathcal{O}_L = \mathfrak{P}_L^6.$$

Observe that $x + \omega^2 y + \omega z = -3\sqrt[3]{\beta}$. Denote

$$\bar{X} := \frac{-x}{3\sqrt[3]{\beta}}, \bar{Y} := \frac{-\omega^2 y}{3\sqrt[3]{\beta}} \text{ and } \bar{Z} := \frac{-\omega z}{3\sqrt[3]{\beta}}.$$

Then,

$$\begin{cases} \bar{X} + \bar{Y} + \bar{Z} = 1 \\ \bar{X}\bar{Y}\bar{Z} = -\alpha(27\beta)^{-1} \in \mathcal{O}^*_{S_K} \end{cases} \tag{24}$$

giving

$$v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta}) = v_{\tilde{\mathfrak{P}}}(27\bar{X}\bar{Y}\bar{Z})$$

Consider τ the element of $\mathrm{Gal}(L/K(\omega))$ such that $\tau(\sqrt[3]{\beta}) = \omega\sqrt[3]{\beta}$. Note that $\tau(\bar{X}) = \bar{Y}$ and $\tau(\bar{Y}) = \bar{Z}$. Moreover, $\tau(\mathfrak{P}_L) = \mathfrak{P}_L$.
Hence we get $v_{\mathfrak{P}_L}(\bar{X}) = v_{\mathfrak{P}_L}(\bar{Y}) = v_{\mathfrak{P}_L}(\bar{Z}) =: s$. If $s > 0$, we would get $\mathfrak{P}_L | 1$ by (24), a contradiction. Thus, we always have $s \leq 0$. By (24) again, we get that $v_{\mathfrak{P}_L}(\bar{X}\bar{Y}\bar{Z}) = 3s$ must be a multiple of 6 as $\bar{X}\bar{Y}\bar{Z} \in \mathcal{O}^*_{S_K}$. Thus $s = 2n$ for $n \leq 0$. Consequently,

$$v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta}) = v_{\tilde{\mathfrak{P}}}(27\bar{X}\bar{Y}\bar{Z}) = 3v_{\tilde{\mathfrak{P}}}(3) + n \leq 3v_{\tilde{\mathfrak{P}}}(3) \text{ as } n \leq 0$$

.
Case (2): If $\beta = \pm 1$ and $\beta \in (\mathcal{O}^*_{S_K})^3$ we have that $[L : K] = 2$ by (23). Standard algebraic number theory gives $\mathcal{O}_L = \mathcal{O}_K(\omega)$. So, by Dedekind Theorem, it follows that

$$(3)\mathcal{O}_L = \mathfrak{P}_L^2.$$

The argument follows exactly as in case (1) from here giving

$$v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta}) = v_{\tilde{\mathfrak{P}}}(27\bar{X}\bar{Y}\bar{Z}) = 3v_{\tilde{\mathfrak{P}}}(3) + m \leq 3v_{\tilde{\mathfrak{P}}}(3) \text{ for an integer } m \leq 0.$$

By symmetry of α and β we get $v_{\tilde{\mathfrak{P}}}(\frac{\beta}{\alpha}) = -v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta}) \leq 3v_{\tilde{\mathfrak{P}}}(3)$ and hence we can conclude the proof by Theorem 1.5 as promised. □

8 Further work

We plan to work further on the two main theorems and the corresponding examples aiming to:

(i) give a more comprehensive set of examples for both the $(p, p, 2)$ and $(p, p, 3)$ case;

(ii) compute the effective constant B_K in some of the cases;

(iii) see if we can find out more about the solutions if we assume the Eichler-Shimura modularity conjecture, for example, find a larger set than $U_{K,\tilde{\mathfrak{P}}}$ on which the asymptotic Fermat holds.

9 Bibliography

References

[1] A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, D. Roe, C. Vincent, M. West. *A robust implementation for solving the S-unit equation and several applications.*

[2] M. A. Bennett and C. M. Skinner. *Ternary Diophantine equations via Galois representations and modular forms.* Canad. J. Math. 56 (2004), no. 1, 23–54.

[3] D. Blasius. *Elliptic curves, Hilbert modular forms, and the Hodge conjecture.* Contributions to automorphic forms, geometry, and number theory, 83–103, Johns Hopkins Univ. Press 2004.

[4] H. Cohen. *Advanced topics in computational number theory*, volume193 of Graduate Texts in Mathematics. Springer-Verlag, New York,2000.

[5] H. Cohen *Number Theory, Volume II: Analytic and Modern Tools.*GTM 240, Springer, 2007.

[6] K. Conrad. *Dirichlet's Unit Theorem.* `https://kconrad.math.uconn.edu/blurbs/gradnumthy/unittheorem.pdf`

[7] H. Darmon. *Rational Points on Modular Elliptic Curves.* CBMS 101, AMS, 2004.

[8] H. Darmon, L. Merel. *Winding quotients and some variants of Fermat's Last Theorem*

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

[10] Derickx M, Najman F, Siksek S. *Elliptic curves over totally real cubic field are modular.*

[11] J.H. Evertse, K. Gyory, C. L. Stewart, R. Tijdeman. *S-unit equations and their applications.* `https://core.ac.uk/download/pdf/301669309.pdf`.

[12] N. Freitas, B. V. Le Hung and S. Siksek. *Elliptic curves over real quadratic fields are modular.*Inventiones Mathematicae 2015; 1 (201): 159-206.

[13] N. Freitas and S. Siksek. *Criteria for irreducibility of mod p representations of Frey curves.* Journal de théorie des nombres de Bordeaux 2015; 1 (27): 67-76.

[14] N. Freitas, S. Siksek. *The Asymptotic Fermat's Last Theorem for Five-Sixths of Real Quadratic Fields.* `https://arxiv.org/pdf/1307.3162.pdf`

[15] K. Fujiwara. *Level optimisation in the totally real case.*arXiv:0602586v1, 27 February 2006.

[16] F. Jarvis. *Level lowering for modular* mod l *representations over totally real fields.* Math. Ann. 313 (1999), no. 1, 141–160.

[17] F. Jarvis. *Correspondences on Shimura curves and Mazur's principle at p.*Pacifc J. Math.,213 (2), 2004, 267–280.

[18] Y. Kara, E. Ozman. *Asymptotic Generalized Fermat's Last Theorem over Number Fields.* International Journal of Number Theory. Vol. 16, No. 05, pp. 907-924 (2020).

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

[20] Angelos Koutsianas. *Applications of S-unit Equations to the Arithmetic of Elliptic Curves* . PhD thesis, University of Warwick, 2016.

[21] E. Işik, y. Kara, e. Ozman. *On ternary Diophantine equations of signature* $(p, p, 2)$ *over number fields.* `https://journals.tubitak.gov.tr/math/issues/mat-20-44-4/mat-44-4-9-1911-88.pdf`

[22] B. Mazur. *Rational isogenies of prime degree.*Inventiones Math. 44 (1978), 129–162.

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

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

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

[26] J-P. Serre. *Abelian l-Adic Representations and Elliptic Curves.* `https://www.math.mcgill.ca/~darmon/courses/18-19/gs/serre-mcgill.pdf`

[27] C. L. Siegel. *Über einige Anwendungen diophantischer Approximationen.* Abh. Preuss. Akad. Wiss. (1929), 1–41.

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

[29] S. Siksek. *The modular approach to diophantine equations.* `http://homepages.warwick.ac.uk/~maseap/papers/ihpnotes7.pdf`.

[30] J.H.Silverman. *The Arithmetic of Elliptic Curves.*, GTM 106, Springer, 1986.

[31] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.*GTM 151, Springer, 1994.

[32] Nigel P. Smart. *The algorithmic resolution of Diophantine equations.* London Mathematical Society Student Texts 41, 1998.

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

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

[35] G. Ţurcaş. *On Serre's modularity conjecture and Fermat's equation over quadratic imaginary field of class number one.* Journal of Number Theory, Volume 209, April 2020, Pages 516-530.

[36] B. de Weger. *Algorithms for Diophantine Equations.* PhD thesis, University of Leiden, 1988.

[37] A. Wiles. *On ordinary* λ*-adic representations associated to modular forms.* Invent. Math. 94 (1988), no. 3, 529–573.

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

[39] S.-W. Zhang. *Heights of Heegner points on Shimura curves.* Ann. of Math. 153 (2001), 27.

Appendix A Solutions to S-unit equations for L/K_2

Using the S-unit solver in Sage by A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, D. Roe, C. Vincent, M. West in [1] we got:

```
L0=NumberField( x^2-26 )
SK-unit solutions of K are
[((0, 0, 1), (1, 0, 0), 2, -1), ((0, 0, -1), (0, 0, -1), 1/2, 1/2)]

L1.<a1>=NumberField( x^4 - 50*x^2 + 729 )
[((3, 0, 2), (2, 0, 0), 2, -1), ((1, 0, -1), (0, 0, -1),
 -1/108*a1^3 + 23/108*a1 + 1/2, 1/108*a1^3 - 23/108*a1 + 1/2),
((1, 0, 0), (3, 0, 1), -1/54*a1^3 + 23/54*a1, 1/54*a1^3 - 23/54*a1 + 1),
((0, 0, 1), (3, 0, 0), -1/54*a1^3 + 23/54*a1 + 1, 1/54*a1^3 - 23/54*a1),
((1, 0, -2), (1, 0, -2), 1/2, 1/2)]

L2.<a2>=NumberField( x^4 - 10*x^2 - 1 )
[((1, 0, 1, 2), (1, 0, 0, 0), 2, -1),
((1, 0, -1, -2), (1, 0, -1, -2), 1/2, 1/2)]

L3.<a3>=NumberField( x^4 - 56*x^2 + 576 )
S-unit solver got a SystemExit error.

L4.<a4>=NumberField( x^4 + 10*x^2 - 1 )
[((1, 0, 1, 2), (1, 0, 0, 0), 2, -1),
((1, 0, -1, -2), (1, 0, -1, -2), 1/2, 1/2)]

L5.<a5>=NumberField( x^4 - 48*x^2 + 784 )
[((1, 0, 1, 2), (1, 0, 0, 0), 2, -1),
((1, 0, -1, -2), (1, 0, -1, -2), 1/2, 1/2)]

L6.<a6>=NumberField( x^4 - 20*x^2 - 4 )
[((0, 1, 0, 2), (1, 0, 0, 0), 2, -1),
((1, 3, 1, 4), (0, 1, 2, 0),a6^3 - 4*a6^2 - 2*a6,
-a6^3 + 4*a6^2 + 2*a6 + 1), ((1, -3, -1, -4), (0, -2, 1, -4),
 -1/16*a6^3 + 11/8*a6 + 1/2, 1/16*a6^3 - 11/8*a6 + 1/2),
((0, -1, -2, 0), (0, 2, -1, 4), a6^3 + 4*a6^2 - 2*a6 + 1,
-a6^3 - 4*a6^2 + 2*a6),((0, -1, 0, -2), (0, -1, 0, -2), 1/2, 1/2)]

L7.<a7>=NumberField( x^4 + 20*x^2 - 4 )
[((0, 1, 0, 2), (1, 0, 0, 0), 2, -1), ((1, 3, 1, 4), (0, 1, 2, 0),
-9*a7^3 - 4*a7^2 - 182*a7 - 80, 9*a7^3 + 4*a7^2 + 182*a7 + 81),
((1, -3, -1, -4), (0, -2, 1, -4), -1/16*a7^3 - 9/8*a7 + 1/2,
1/16*a7^3 + 9/8*a7 + 1/2),((0, -1, -2, 0), (0, 2, -1, 4),
```

```
−9*a7^3 + 4*a7^2 − 182*a7 + 81, 9*a7^3 − 4*a7^2 + 182*a7 − 80),
((0, −1, 0, −2), (0, −1, 0, −2), 1/2, 1/2)]
```

Appendix B Solutions to S-unit equations for L/K_3

L_0, L_1, L_4, L_5, L_7 are computed using the open-source S-unit solver in Sage by A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, D. Roe, C. Vincent, M. West in [1].
L_2, L_3, L_6 are computed using Benjamin Matschke's S-unit solver which can be found at `https://github.com/bmatschke/s-unit-equations`.

```
L0=NumberField( x^2−35 )
[((0, 0, 1), (1, 0, 0), 2, −1), ((0, 0, −1), (0, 0, −1), 1/2, 1/2)]

L1.<a1>=NumberField( x^4 − 68*x^2 + 1296 )
[((3, 0, 2), (2, 0, 0), 2, −1), ((0, 0, −1), (1, 0, −1),
−1/144*c^3 + 2/9*c + 1/2, 1/144*c^3 − 2/9*c + 1/2),
((1, 0, 0), (3, 0, 1), 1/72*c^3 − 4/9*c, −1/72*c^3 + 4/9*c + 1),
((0, 0, 1), (3, 0, 0), 1/72*c^3 − 4/9*c + 1, −1/72*c^3 + 4/9*c),
((1, 0, −2), (1, 0, −2), 1/2, 1/2)]

L2.<a2>=NumberField( x^4 − 12*x^2 + 1 )
S−unit solver got a SystemExit error.

[
    "−14*x^3 + 48*x^2 + 2*x − 3",
    "2",
    "5/4*x^3 − 59/4*x + 1/2",
    "1/2",
    "1/4*x^3 − 7/4*x + 1/2",
    "−4*x^3 + 52*x − 15",
    "1/8*x^3 − 13/8*x + 1/2",
    "−166*x^3 − 48*x^2 + 1978*x + 573",
    "166*x^3 + 48*x^2 − 1978*x − 572",
    "−1/8*x^3 + 13/8*x + 1/2",
    "−1/4*x^3 + 7/4*x + 1/2",
    "−5/4*x^3 + 59/4*x + 1/2",
    "−4*x^3 + 52*x + 16",
    "−14*x^3 − 48*x^2 + 2*x + 4",
    "−166*x^3 + 48*x^2 + 1978*x − 572",
    "4*x^3 − 52*x + 16",
    "14*x^3 − 48*x^2 − 2*x + 4",
    "14*x^3 + 48*x^2 − 2*x − 3",
```

```
    "4*x^3 - 52*x - 15",
    "-1",
    "166*x^3 - 48*x^2 - 1978*x + 573"
  ]
L3.<a3>=NumberField( x^4 - 74*x^2 + 1089 )
S-unit solver got a SystemExit error.

"set of values for x": [
    "2",
    "1/132*a3^3 - 41/132*a3 + 1",
    "1/2",
    "-1/132*a3^3 + 41/132*a3 + 1/2",
    "-1/33*a3^3 + 41/33*a3 + 4",
    "-1/264*a3^3 + 41/264*a3 + 1/2",
    "1/33*a3^3 - 41/33*a3 - 3",
    "1/33*a3^3 - 41/33*a3 + 4",
    "-1/33*a3^3 + 41/33*a3 - 2",
    "1/264*a3^3 - 41/264*a3 + 1/2",
    "-2/11*a3^3 + 82/11*a3 + 17",
    "2/11*a3^3 - 82/11*a3 + 17",
    "1/66*a3^3 - 41/66*a3",
    "1/33*a3^3 - 41/33*a3 + 3",
    "1/176*a3^3 - 41/176*a3 + 1/2",
    "2/11*a3^3 - 82/11*a3 - 16",
    "-1/132*a3^3 + 41/132*a3",
    "1/132*a3^3 - 41/132*a3 + 1/2",
    "-1/66*a3^3 + 41/66*a3 + 2",
    "1/66*a3^3 - 41/66*a3 + 2",
    "-1/66*a3^3 + 41/66*a3 - 1",
    "-1/66*a3^3 + 41/66*a3 + 1",
    "-1/176*a3^3 + 41/176*a3 + 1/2",
    "1/33*a3^3 - 41/33*a3 - 2",
    "-2/11*a3^3 + 82/11*a3 - 16",
    "-1/33*a3^3 + 41/33*a3 - 3",
    "-1/66*a3^3 + 41/66*a3",
    "1/66*a3^3 - 41/66*a3 + 1",
    "1/132*a3^3 - 41/132*a3",
    "1/66*a3^3 - 41/66*a3 - 1",
    "-1/33*a3^3 + 41/33*a3 + 3",
    "-1/132*a3^3 + 41/132*a3 + 1",
    "-1"
  ]
```

```
L4.<a4>=NumberField( x^4 + 12*x^2 + 1 )
[((0, 0, 1), (1, 0, 0), 2, -1), ((0, 0, -1), (0, 0, -1), 1/2, 1/2)]

L5.<a5>=NumberField( x^4 - 66*x^2 + 1369 )
[((1, 0, 2), (1, 0, 0), 2, -1), ((1, 0, -2), (1, 0, -2), 1/2, 1/2)]

L6.<a6>=NumberField( x^4 - 24*x^2 + 4 )
S-unit solver got a SystemExit error.

"set of values for x": [
    "2",
    "1/8*a6^2 + 3/4*a6 + 3/4",
    "-1/8*a6^2 + 3/4*a6 + 1/4",
    "-39/4*a6^3 + 4*a6^2 + 465/2*a6 - 95",
    "-a6^3 + 22*a6 + 9",
    "3/4*a6^3 + 1/4*a6^2 - 18*a6 - 13/2",
    "-3/16*a6^3 - 1/8*a6^2 + 39/8*a6 + 2",
    "3/4*a6^3 + 1/4*a6^2 - 18*a6 - 11/2",
    "3/16*a6^3 + 1/8*a6^2 - 39/8*a6 - 1",
    "3/8*a6^3 + 1/8*a6^2 - 9*a6 - 11/4",
    "a6^3 - 22*a6 + 9",
    "59/4*a6^3 + 6*a6^2 - 703/2*a6 - 143",
    "-3/4*a6^3 + 1/4*a6^2 + 18*a6 - 13/2",
    "-3/4*a6^3 + 1/4*a6^2 + 18*a6 - 11/2",
    "-3/16*a6^3 + 1/8*a6^2 + 39/8*a6 - 1",
    "-3/8*a6^3 + 1/8*a6^2 + 9*a6 - 11/4",
    "39/4*a6^3 + 4*a6^2 - 465/2*a6 - 95",
    "-1/4*a6^3 + 11/2*a6 - 1",
    "-1/4*a6^3 + 11/2*a6 - 2",
    "3/64*a6^3 - 39/32*a6 + 1/2",
    "-1/8*a6^3 + 11/4*a6 - 1/2",
    "1/4*a6^3 - 11/2*a6 - 2",
    "1/4*a6^3 - 11/2*a6 - 1",
    "1/8*a6^3 - 11/4*a6 - 1/2",
    "39/4*a6^3 - 4*a6^2 - 465/2*a6 + 96",
    "-59/4*a6^3 - 6*a6^2 + 703/2*a6 + 144",
    "-59/4*a6^3 + 6*a6^2 + 703/2*a6 - 143",
    "1/2",
    "5/4*a6^3 + 6*a6^2 - 1/2*a6",
    "-12*a6^3 + 312*a6 + 128",
    "3/4*a6^3 + 4*a6^2 + 3/2*a6",
    "-1/4*a6^2 - 3/2*a6 - 1/2",
    "-5/4*a6^3 + 6*a6^2 + 1/2*a6",
```

```
"-3/64*a6^3 + 39/32*a6 + 1/2",
"-1/8*a6^3 + 5/4*a6 + 1/2",
"-1/4*a6^3 + 11/2*a6 + 3",
"-1/4*a6^3 + 11/2*a6 + 2",
"-1/8*a6^3 + 11/4*a6 + 1/2",
"3/4*a6^3 - 4*a6^2 + 3/2*a6 + 1",
"-1/8*a6^3 + 11/4*a6 + 3/2",
"-5/4*a6^3 - 6*a6^2 + 1/2*a6 + 1",
"12*a6^3 - 312*a6 - 127",
"-3/4*a6^3 - 4*a6^2 - 3/2*a6 + 1",
"5/4*a6^3 - 6*a6^2 - 1/2*a6 + 1",
"-3/4*a6^3 + 4*a6^2 - 3/2*a6",
"-1/16*a6^3 + 11/8*a6 + 1/4",
"1/4*a6^3 - 11/2*a6 + 2",
"-1/16*a6^3 + 11/8*a6 + 3/4",
"-1/16*a6^3 + 11/8*a6 + 1/2",
"1/4*a6^3 - 11/2*a6 + 3",
"59/4*a6^3 - 6*a6^2 - 703/2*a6 + 144",
"1/8*a6^3 - 11/4*a6 + 1/2",
"1/8*a6^3 - 11/4*a6 + 3/2",
"-39/4*a6^3 - 4*a6^2 + 465/2*a6 + 96",
"-1/4*a6^2 + 3/2*a6 - 1/2",
"1/8*a6^3 - 5/4*a6 + 1/2",
"1/4*a6^2 - 3/2*a6 + 3/2",
"1/16*a6^3 - 11/8*a6 + 1/4",
"1/16*a6^3 - 11/8*a6 + 1/2",
"1/16*a6^3 - 11/8*a6 + 3/4",
"-1/4*a6^2 - 3/2*a6 + 1/2",
"1/4*a6^2 - 3/2*a6 + 1/2",
"1/8*a6^2 - 3/4*a6 + 3/4",
"3/4*a6^3 - 1/4*a6^2 - 18*a6 + 13/2",
"-a6^3 + 22*a6 - 8",
"3/4*a6^3 - 1/4*a6^2 - 18*a6 + 15/2",
"-1/8*a6^2 - 3/4*a6 + 1/4",
"-12*a6^3 + 312*a6 - 127",
"a6^3 - 22*a6 - 8",
"3/8*a6^3 - 1/8*a6^2 - 9*a6 + 15/4",
"-7/8*a6^3 + 83/4*a6 + 1/2",
"3/16*a6^3 - 1/8*a6^2 - 39/8*a6 + 2",
"12*a6^3 - 312*a6 + 128",
"-3/4*a6^3 - 1/4*a6^2 + 18*a6 + 15/2",
"-3/4*a6^3 - 1/4*a6^2 + 18*a6 + 13/2",
"7/8*a6^3 - 83/4*a6 + 1/2",
"-1",
```

```
    "1/4*a6^2 + 3/2*a6 + 3/2",
    "-1/4*a6^2 + 3/2*a6 + 1/2",
    "1/4*a6^2 + 3/2*a6 + 1/2",
    "-3/8*a6^3 - 1/8*a6^2 + 9*a6 + 15/4"]

L7.<a7>=NumberField( x^4 + 24*x^2 + 4 )
[((1, 0, 2), (1, 0, 0), 2, -1), ((1, 0, -2), (1, 0, -2), 1/2, 1/2)]
```