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 $Aa^p + Bb^q = Cc^r$ over K. We call the triple of exponents (p, q, r) the *signature* of the equation. We prove various results concerning the solutions to the Fermat equation with signature $(p, p, 2)$ and $(p, p, 3)$ using a method involving modularity, level lowering and image of inertia comparison. These generalize and extend the recent work of Işik, Kara and Ozman. For example, consider K a totally real field of degree n with $2 \nmid h_K^+$ and 2 inert. Moreover, suppose there is a prime $q \geq 5$ which totally ramifies in K and satisfies $\gcd(n, q-1) = 1$, then we know that the equation $a^p + b^p = c^2$ has no primitive, non-trivial solutions $(a, b, c) \in \mathcal{O}_K^3$ with $2|b$ for p sufficiently large.

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" [34]. 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 level lowering 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 [25].

Even before Wiles announced his proof, various generalizations of Fermat's Last Theorem had already been considered, which are 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 [16], Işik, Kara and Ozman list all known cases where equation (1) has been solved over the rational integers in two tables (p.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 (n, n, k) where $k \in \{2, 3\}$. Darmon and Merel [6] and Poonen [19] proved the following theorem:

Theorem 1 (Darmon and Merel)**.** *(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 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 [18] and modular by Wiles and Taylor [34] and [29]. Applying Ribet's level lowering theorem [21] one gets that 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 [6], 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 [19].

Recently, important progress has been done towards generalisation of the modularity approach over larger number fields. In [12] 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 [7] extended the results of Freitas and Siksek [12] 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 [24] 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 [15] to the case of the generalized Fermat equation. Also, recently in [30] and [31] Ţurcaş studied Fermat equation over imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ with class number one.

We now present a result by Işik, Kara and Ozman, proved in [16] which serves as the starting point of this paper. 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:

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

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

where $f(\mathfrak{P}/2)$ denotes the residual degree of $\mathfrak{P}$.

Theorem 2 (Işik, Kara and Ozman)**.** *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 constant 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).

1.2 Our results

We start by using the methods pioneered by Freitas and Siksek in [12] involving modularity, level lowering and image of inertia comparison to generalize Işik, Kara and Ozman's Theorem 2. More precisely, we relax the assumption on the class group from $h_K^+ = 1$ to $Cl_{S_K}(K)[2] = \{1\}$. We 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. Note that when all $\mathfrak{P} \in S$ are principal, $Cl_S(K)$ is the usual $Cl(K)$, and hence we will drop the S in the notation. Moreover, in this case, $Cl(K)[p] = \{1\}$ is equivalent to $p \nmid h_K$, for p prime.

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

Theorem 3 (Main Theorem for $(p, p, 2)$)**.** *Let K be a totally real number field with $Cl_{S_K}(K)[2] = \{1\}$ where $S_K := \{\mathfrak{P} : \mathfrak{P}$ is a prime of K above $2\}$. Suppose that there exists some distinguished prime $\tilde{\mathfrak{P}} \in S_K$, such that every solution $(\alpha, \beta, \gamma) \in \mathcal{O}_{S_K}^* \times \mathcal{O}_{S_K}^* \times \mathcal{O}_{S_K}$ to the equation*

$$\alpha + \beta = \gamma^2$$

satisfies $|v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta})| \leq 6v_{\tilde{\mathfrak{P}}}(2)$. Then, there is a constant 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 primitive, non-trivial solutions $(a, b, c) \in \mathcal{O}_K^3$ with $\tilde{\mathfrak{P}}|b$.

Remark 4. By Theorem 41 the equation

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

has finitely many solutions up to scaling by a square in $\mathcal{O}_{S_K}^*$, and these are effectively computable. Hence the criteria in Theorem 3 is testable in finite time.

Imposing local constraints, we get that for a totally real number field, in which 2 is inert, the following holds:

Theorem 5. *Let K be a totally real number field with $2 \nmid h_K^+$ in which 2 is inert. Let $\mathfrak{P}$ be the only prime above 2, and hence $S_K = \{\mathfrak{P}\}$. Suppose that every solution $(\alpha, \gamma) \in \mathcal{O}_{S_K}^* \times \mathcal{O}_{S_K}$ with $v_{\mathfrak{P}}(\alpha) \geq 0$ to the equation*

$$\alpha + 1 = \gamma^2 \tag{2}$$

satisfies $v_{\mathfrak{P}}(\alpha) \leq 6$. *Then, there is a constant* 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 primitive, non-trivial solutions* $(a, b, c) \in \mathcal{O}_K^3$ *with* $2|b$.

More concretely, for quadratic totally real number fields K, Theorem 5 becomes:

Theorem 6. *Let* $d > 5$ *be a rational prime satisfying* $d \equiv 5 \mod 8$. *Write* $K = \mathbb{Q}(\sqrt{d})$. *Then, there is a constant* 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 primitive, non-trivial solutions* $(a, b, c) \in \mathcal{O}_K^3$ *with* $2|b$.

More generally, by employing additional local information, the following holds.

Theorem 7. *Let* K *be a totally real field of degree* n*, and let* $q \geq 5$ *be a rational prime. Suppose*

(i) $2 \nmid h_K^+$,

(ii) $\gcd(n, q-1) = 1$,

(iii) 2 *is inert in* K,

(iv) q *totally ramifies in* K.

Then, there is a constant 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 primitive, non-trivial solutions* $(a, b, c) \in \mathcal{O}_K^3$ *with* $2|b$.

Remark 8. A few examples of totally real fields K satisfying the conditions above are the degree 3 extensions which are the splitting fields of: $p_1(x) = x^3 - 51x - 85$, $p_2(x) = x^3 - x^2 - 40x + 13$, $p_3(x) = x^3 - x^2 - 38x - 75$ and $p_4(x) = x^3 - 17x - 17$.

We use the same methods to study the asymptotic behaviour of the analogue $(p, p, 3)$ equation and we get the following:

Theorem 9 (Main Theorem for $(p, p, 3)$)**.** *Let* K *be a totally real number field with* $Cl_{S_K}(K)[3] = \{1\}$ *where* $S_K := \{\mathfrak{P} : \mathfrak{P}$ *is a prime of* K *above* $3\}$. *Suppose that there exists some distinguished prime* $\tilde{\mathfrak{P}} \in S_K$ *such that every solution* $(\alpha, \beta, \gamma) \in \mathcal{O}_{S_K}^* \times \mathcal{O}_{S_K}^* \times \mathcal{O}_{S_K}$ *to the* S_K *equation*

$$\alpha + \beta = \gamma^3$$

satisfies $|v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta})| \leq 3v_{\tilde{\mathfrak{P}}}(3)$. *Then, there is a constant* 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 primitive, non-trivial solutions* $(a, b, c) \in \mathcal{O}_K^3$ *with* $\tilde{\mathfrak{P}}|b$.

Remark 10. By Theorem 41 the equation

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

has finitely many solutions up to scaling by a cube in $\mathcal{O}_{S_K}^*$, and these are effectively computable. Hence the criteria in Theorem 9 is testable in finite time.

Similarly to the $(p,p,2)$ case, the following hold when employing local information. We will consider various field extensions involving the primitive cube root of unity $\omega := \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$.

Theorem 11. *Let K be a totally real number field such that $3 \nmid h_{K(\omega)}$, $3 \nmid h_K$ and in which 3 is inert. Let $\mathfrak{P}$ be the only prime above 3, and hence $S_K = \{\mathfrak{P}\}$. Suppose that every solution $(\alpha, \gamma) \in \mathcal{O}_{S_K}^* \times \mathcal{O}_{S_K}$ with $v_{\mathfrak{P}}(\alpha) \geq 0$ to the equation*

$$\alpha + 1 = \gamma^3 \tag{3}$$

satisfies $v_{\mathfrak{P}}(\alpha) \leq 3$. Then, there is a constant 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 primitive, non-trivial solutions $(a,b,c) \in \mathcal{O}_K^3$ with $3|b$.

Theorem 12. *Let d a positive, square-free satisfying $d \equiv 2 \mod 3$. Write $K = \mathbb{Q}(\sqrt{d})$ and suppose $3 \nmid h_{K(\omega)}$, $3 \nmid h_K$. Then, there is a constant 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 primitive, non-trivial solutions $(a,b,c) \in \mathcal{O}_K^3$ with $3|b$.*

Theorem 13. *Let K be a totally real field of degree n, and let $q \geq 5$ be a rational prime. Suppose*

(i) $3 \nmid h_{K(\omega)}$ *and* $3 \nmid h_K$,

(ii) $\gcd(n, q^2 - 1) = 1$,

(iii) 3 *is inert in K,*

(iv) q *totally ramifies in K.*

Then, there is a constant 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 primitive, non-trivial solutions $(a,b,c) \in \mathcal{O}_K^3$ with $3|b$.

Remark 14. A few examples of totally real fields K satisfying the conditions above are the degree 5 extensions which are the splitting fields of: $p_1(x) = x^5 - 25x^3 - 10x^2 + 50x - 20$, $p_2(x) = x^5 - 30x^3 - 20x^2 + 160x + 128$, $p_3(x) = x^5 - 15x^3 - 10x^2 + 10x + 4$ and $p_4(x) = x^5 - 20x^3 - 15x^2 + 10x + 4$.

1.3 Notational conventions

We will follow the notational conventions in [12]. 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 ϖ will denote a prime of $\mathbb{Q}_{\mathfrak{f}}$ above p; of course if $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$ we write p instead of ϖ. All other primes we consider are primes of K. We reserve the symbol $\mathfrak{P}$ for primes belonging to S. 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 $\mathfrak{q}$.

Acknowledgments. I am sincerely grateful to my supervisor Samir Siksek for his continuous support, useful comments and reviewing this paper.

2 Preliminaries

2.1 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 15. *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 has a model of the form

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

Moreover, there is a bijection between

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

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

(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

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

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

Proof. (i) The first part is a well-known result. 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) If E is in Weierstrass form we can translate the K-torsion point to $(0, 0)$. This will give a model of the form

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

We now impose the condition that $(0, 0)$ has order 3. First, we compute $-(0, 0) = (0, -a_3)$ and note that we require $(0, 0) \neq -(0, 0) = (0, -a_3)$, 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,

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

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 16. *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* $E \to \mu := \lambda - 4 \in \mathcal{O}_S^*$, *where λ is as in Lemma 15 (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* $E \to \mu := \lambda - 27 \in \mathcal{O}_S^*$, *where λ is as in Lemma 15 (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 15 (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 15 (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).

□

We say that a fractional ideal is an S-ideal if its decomposition into primes contains only primes in S.

Lemma 17. *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) Suppose S contains the primes above 2 and E has a K-torsion point of order 2. Let $(\lambda, \mu) \in \mathcal{O}_S \times \mathcal{O}_S^*$ correspond to E as in Lemma 16 (i) and therefore satisfy $\lambda - \mu = 4$. Then $(\lambda)\mathcal{O}_K = I^2 J$ where I, J are fractional ideals with J being an S-ideal.

(ii) Suppose S contains the primes above 3 and E has a K-torsion point of order 3. Let $(\lambda, \mu) \in \mathcal{O}_S \times \mathcal{O}_S^*$ correspond to E as in Lemma 16 (ii) and therefore satisfy $\lambda - \mu = 27$. Then $(\lambda)\mathcal{O}_K = I^3 J$ where I, J are fractional ideals with J being an S-ideal.

Proof. (i) By Lemma 15 (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

the minimal discriminant of an elliptic curve which can be found in [26, Ch. 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 15 (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 the minimal discriminant of an elliptic curve which can be found in [26, Ch. 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.

□

2.2 Modularity Results

We now carefully formulate modularity in the context of a totally real field. Let us 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' [33].

We need the following theorem proved by Freitas, Hung and Siksek in [9]:

Theorem 18. *Let K be a totally real field. There are at most finitely many $\bar{K}$-isomorphism classes of 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 [8]:

Theorem 19. *Let K be a totally real cubic number field and E be an elliptic curve over K. Then E is modular.*

2.3 Irreductibility of $\mod p$ representations of elliptic curves

We need the following theorem in the level lowering step of our proof. This was proved in [11, Theorem 2] and it is derived from the work of David and Momose who in turn built on Merel's Uniform Boundedness Theorem.

Theorem 20. *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.*

Remark 21. The above theorem is also true for any totally real field by replacing K by its Galois closure.

2.4 Level lowering

We present a level lowering result proved by Freitas and Siksek in [12] derived from the work of Fujira [13], Jarvis [14], and Rajaei [20]. 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 22. *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* $\mathbb{Q}(\zeta_p)^+ \not\subseteq K$,

(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 ϖ of $\mathbb{Q}_{\mathfrak{f}}$ such that $\varpi|p$ and $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$.

Proof. A proof is given in [12, p. 8]. □

2.5 Eichler-Shimura

For totally real fields, modularity reads as follows.

Conjecture 23 (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 $\mathfrak{f}$.

Freitas and Siksek obtain the following theorem [12] from works of Blasius [3], Darmon [5] and Zhang [35].

Theorem 24. *Let E be an elliptic curve over a totally real field K , and p be an odd prime. Suppose that $\overline{\rho}_{E,p}$ is irreducible, and $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ 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 $\mathfrak{f}$.

3 Signature $(p, p, 2)$

Let K be a totally real field. Recall the set $S_K = \{\mathfrak{P} : \mathfrak{P} \text{ is a prime of } K \text{ above } 2\}$. Throughout this section we denote by $(a, b, c) \in \mathcal{O}_K^3$ a non-trivial, primitive solution of $a^p + b^p = c^2$.

3.1 Frey Curve

For $(a, b, c) \in \mathcal{O}_K^3$ as described above we associate the following Frey elliptic curve defined over K:

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

We 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 25. *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*

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

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, the model is minimal at $\mathfrak{q}$ and has multiplicative reduction. Hence $p|v_\mathfrak{q}(\Delta_E) = v_\mathfrak{q}(\Delta_\mathfrak{q})$. On the other hand $\mathfrak{P} \in S_K$ is an even prime, so we have $r_\mathfrak{P} = v_\mathfrak{P}(\mathcal{N}_E) \leq 2 + 6v_\mathfrak{P}(2)$ by [27, 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 26. *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 18, 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 $\lambda := b^p/a^p$. The j-invariant of E is

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

We can assume $\lambda \notin \{0, \pm 1\}$ as these λ lead to $j(\lambda) \in \mathbb{Q}$ and we know that all rational elliptic curves are modular. Each equation $j(\lambda) = j_i$ has at most three solutions $\lambda \in K$. Thus there are values $\lambda_1, \ldots, \lambda_m \in K$ (where $m \leq 3n$) 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 27. The constant A_K is ineffective as the finiteness of Theorem 18 relies on Falting's Theorem (which is ineffective). See [9] for more details. Note that if K is quadratic or cubic we get $A_K = 0$ (by the last part of Theorem 18 and Theorem 19).

□

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 24 and for controlling the behaviour at the primes in S_K of the newform obtained by level lowering.

Lemma 28. *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 [12, Lemma 3.4]. □

Lemma 29. *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 28, 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, $v_q(j_E) = -pv_{\mathfrak{q}}(a^2 b)$, i.e. $p | v_{\mathfrak{q}}(j_E)$. □

Lemma 30. *Let $\mathfrak{P} \in S_K$ and (a, b, c) a non-trivial, primitive solution to $a^p + b^p = c^2$ with $\mathfrak{P} | b$ and prime exponent $p > 6v_{\mathfrak{P}}(2)$. 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 $v_{\mathfrak{P}}(j_E) = 6v_{\mathfrak{P}}(2) - pk$. Since $p > 6v_{\mathfrak{P}}(2)$, 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 28 we get $p | \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$. □

3.3 Level Lowering and Eichler Shimura

This is a key result in the proof of Theorem 3, for which we have prepared the ingredients in the previous sections. We will follow the corresponding proofs in [12] and [16].

Theorem 31. *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. Suppose $(a, b, c) \in \mathcal{O}_K^3$ is a non-trivial, primitive solution to $a^p + b^p = c^2$ with prime exponent $p > B_K$ such that $\tilde{\mathfrak{P}} | b$. 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 25 that E has multiplicative reduction outside S_K. By taking B_K sufficiently large, we see from Lemma 26 that E is modular and by Theorem 20 that $\overline{\rho}_{E,p}$ is irreducible. Applying Theorem 22 and Lemma 25 we see that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ for a Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}_p$ and some prime $\varpi | p$ 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], [4, 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 30 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 Theorem 24 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).

To prove (iii) we use that $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$ for some E'/K with conductor $\mathcal{N}_p$. After enlarging B_K by an effective amount, and possibly replacing E' by an

isogenous curve, we may assume that E' has full 2-torsion. This uses standard ideas which can be found, for example, in [22, Section IV-6].

Now let $j_{E'}$ be the j-invariant of E'. As we have already seen, Lemma 30 implies $p|\#\overline{\rho}_{E,p}(I_{\tilde{\mathfrak{P}}})$, hence $p|\#\overline{\rho}_{E',p}(I_{\tilde{\mathfrak{P}}})$, thus by Lemma 28 we get that E' has multiplicative reduction at $\tilde{\mathfrak{P}}$ and so $v_{\tilde{\mathfrak{P}}}(j_{E'}) < 0$. □

3.4 Proof of Theorem 3

Proof. So far, we have shown that for a primitive, non-trivial solution (a, b, c) such that $\tilde{\mathfrak{P}}|b$ with a prime exponent p we associate the Frey elliptic curve in (11). By Theorem 31 for there exists B_K such that for all $p > B_K$ 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 15 (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 31 (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 17 (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

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

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 $v_{\tilde{\mathfrak{P}}}(j_{E'}) \geq 0$, contradicting Theorem 31 (iv) and hence we can conclude the proof. By using (13) we can rewrite the assumption $|v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta})| \leq 6v_{\tilde{\mathfrak{P}}}(2)$ in terms of the valuation of μ, using that $\frac{\alpha}{\beta} = \frac{\mu}{4}$:

$$-4v_{\tilde{\mathfrak{P}}}(2) \leq v_{\tilde{\mathfrak{P}}}(\mu) \leq 8v_{\tilde{\mathfrak{P}}}(2).$$

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. □

3.5 Proof of Theorem 5

Proof. We want to apply Theorem 3 with $\tilde{\mathfrak{P}} = \mathfrak{P}$ and $S_K = \{\mathfrak{P}\}$. Note that $2 \nmid h_K^+$ implies that $Cl_{S_K}(K)[2]$ is trivial. As 2 is inert, we get $v_{\mathfrak{P}}(2) = 1$.

Now, let us consider the equation $\alpha + \beta = \gamma^2$, with $\alpha, \beta \in \mathcal{O}_{S_K}^*$. By scaling the equation by even powers of 2 and swapping α and β if necessary, we may assume $0 \leq v_{\mathfrak{P}}(\beta) \leq v_{\mathfrak{P}}(\alpha)$ with $v_{\mathfrak{P}}(\beta) \in \{0, 1\}$.

Case (1): Suppose $v_{\mathfrak{P}}(\beta) = 1$. If $v_{\mathfrak{P}}(\alpha) \geq 2$, then $v_{\mathfrak{P}}(\gamma^2) = v_{\mathfrak{P}}(\alpha + \beta) = 1$, which leads to a contradiction as $v_{\mathfrak{P}}(\gamma^2)$ must be even. Thus, $v_{\mathfrak{P}}(\alpha) = v_{\mathfrak{P}}(\beta) = 1$ and $v_{\mathfrak{P}}(\frac{\alpha}{\beta}) = 0 \leq 6$.

Case (2): Suppose $v_{\mathfrak{P}}(\beta) = 0$ with β not a square. If $v_{\mathfrak{P}}(\alpha) > 6$, then $v_{\mathfrak{P}}(\gamma^2) = v_{\mathfrak{P}}(\alpha + \beta) = 0$ and $\beta \equiv \gamma^2 \mod 2^6$. Consider the field extension $L = K(\sqrt{\beta})$. We will show that L is unramified at 2, hence contradicting $2 \nmid h_K^+$. Consider the element $\delta := \frac{\gamma + \sqrt{\beta}}{2}$. Its minimal polynomial is

$$m_\delta(X) = X^2 - \gamma X + \frac{\gamma^2 - \beta}{4}.$$

This belongs to $\mathcal{O}_K[X]$ and has odd discriminant $\Delta = \beta$, proving that L is unramified at 2. Thus, we must have $v_{\mathfrak{P}}(\alpha) \leq 6$, giving $v_{\mathfrak{P}}(\frac{\alpha}{\beta}) = v_{\mathfrak{P}}(\alpha) \leq 6$.

Case (3): Suppose β is a square. By dividing everything through β, we may assume $\beta = 1$. Then, by the hypothesis of the theorem we get $v_{\mathfrak{P}}(\frac{\alpha}{\beta}) = v_{\mathfrak{P}}(\alpha) \leq 6$.

All of the possible three cases lead to $v_{\mathfrak{P}}(\frac{\alpha}{\beta}) \leq 6 = 6v_{\mathfrak{P}}(2)$, so we can conclude the proof by Theorem 3. □

3.6 Proof of Theorem 6

Proof. Note that the assumption $d \equiv 5 \mod 8$ gives that 2 is inert in the quadratic field $K = \mathbb{Q}(\sqrt{d})$, take $\mathfrak{P}$ to be the unique prime above 2 and denote $S_K = \{\mathfrak{P}\}$. Moreover, d prime is equivalent to $2 \nmid h_K^+$ by [17, Section 1.3.1]. By Theorem 5 it is enough to check that every solution $(\alpha, \gamma) \in \mathcal{O}_{S_K}^* \times \mathcal{O}_{S_K}$ with $v_{\mathfrak{P}}(\alpha) \geq 0$ to the equation $\alpha + 1 = \gamma^2$ satisfies $v_{\mathfrak{P}}(\alpha) \leq 6$. Rearranging the above we get that $(\gamma + 1)(\gamma - 1) = \alpha$. Denote $x = \frac{(\gamma+1)}{2}$ and $y = \frac{(1-\gamma)}{2}$. Note that since $(\gamma + 1), (\gamma - 1) \in \mathcal{O}_{S_K}$ and they are factors of the S_K-unit α, they must be S_K-units, consequently $x, y \in \mathcal{O}_{S_K}^*$.

In [12, p. 15], it is proved that the only solutions of S_K-unit equation $x + y = 1$, where $K = \mathbb{Q}(\sqrt{d})$ with $d \equiv 5 \mod 8$, $d > 5$ and $S_K = \{\mathfrak{P}\}$ are the so-called *irrelevant* solutions $(-1, 2)$,$(1/2, 1/2)$, $(2, -1)$. This leads to $\alpha \in \{-1, 8\}$, and hence $v_{\mathfrak{P}}(\alpha) \in \{0, 3\}$, proving $v_{\mathfrak{P}}(\alpha) \leq 6$. Hence we can conclude the proof by Theorem 5. □

3.7 Proof of Theorem 7

Proof. We will take $\mathfrak{P}$ to be the unique prime above 2 and denote $S_K = \{\mathfrak{P}\}$. By Theorem 5 it is enough to check that every solution $(\alpha, \gamma) \in \mathcal{O}_{S_K}^* \times \mathcal{O}_{S_K}$ with $v_{\mathfrak{P}}(\alpha) \geq 0$ to the equation $\alpha + 1 = \gamma^2$ satisfies $v_{\mathfrak{P}}(\alpha) \leq 6$. Rearranging as in (3.6) we get an S_K-unit equation $x + y = 1$ such that $\alpha = -4xy$.

We will now use a result proved in [10, p.5]. saying that if K satisfies the hypothesis of Theorem 7, it follows that every solution (x, y) of the S_K-unit

equation satisfies $\max\{v_{\mathfrak{P}}(x), v_{\mathfrak{P}}(y)\} < 2v_{\mathfrak{P}}(2) = 2$. Thus,

$$v_{\mathfrak{P}}(\alpha) = 2v_{\mathfrak{P}}(2) + v_{\mathfrak{P}}(x) + v_{\mathfrak{P}}(y) < 2 + 2 + 2 = 6.$$

Hence we can conclude the proof by Theorem 5. □

4 Signature $(p, p, 3)$

Let K be a totally real field. Recall the set $S_K = \{\mathfrak{P} : \mathfrak{P} \text{ is a prime of } K \text{ above } 3\}$. Throughout this section we denote by $(a, b, c) \in \mathcal{O}_K^3$ a non-trivial, primitive solution of $a^p + b^p = c^3$.

4.1 Frey Curve

For $(a, b, c) \in \mathcal{O}_K^3$ as described above we associate the following Frey elliptic curve defined over K:

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

We compute the arithmetic invariants:

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

Lemma 32. *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*

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

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

Proof. The proof follows exactly like the proof of Lemma 25. □

Lemma 33. *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 follows exactly like the proof of Lemma 26. □

4.2 Images of Inertia

Lemma 34. *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 $p \ge 5$, 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 follows exactly like the proof of Lemma 29. □

Lemma 35. *Let $\mathfrak{P} \in S_K$ and (a, b, c) with $\mathfrak{P}|b$ and 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 30. □

4.3 Level Lowering and Eichler Shimura

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

Theorem 36. *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. Suppose $(a,b,c) \in \mathcal{O}_K^3$ is a non-trivial, primitive solution to $a^p + b^p = c^3$ with prime exponent $p > B_K$ such that $\tilde{\mathfrak{P}} | b$. 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 31. □

4.4 Proof of Theorem 9

Proof. So far, we have shown that for a primitive, non-trivial solution (a,b,c) such that $\tilde{\mathfrak{P}} | b$ with a prime exponent p we associate the Frey elliptic curve in (14). By Theorem 36 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 15 (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 31 (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 17 (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

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

Now, suppose that there is some $\tilde{\mathfrak{P}} \in S_K$ that satisfies $|v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta})| \leq 3 v_{\tilde{\mathfrak{P}}}(3)$. We will show that $v_{\tilde{\mathfrak{P}}}(j_{E'}) \geq 0$, contradicting Theorem 36 (iv) and hence we can

conclude the proof. By using (16) we can rewrite the assumption $|v_{\tilde{\mathfrak{P}}}(\frac{\alpha}{\beta})| \leq 3v_{\tilde{\mathfrak{P}}}(3)$ in terms of the valuation of μ, using that $\frac{\alpha}{\beta} = \frac{\mu}{27}$:

$$0 \leq v_{\tilde{\mathfrak{P}}}(\mu) \leq 6v_{\tilde{\mathfrak{P}}}(3).$$

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. □

4.5 Proof of Theorem 11

Proof. We want to apply Theorem 9 with $\tilde{\mathfrak{P}} = \mathfrak{P}$ and $S_K = \{\mathfrak{P}\}$. As 3 is inert, we get $v_{\mathfrak{P}}(3) = 1$.

Now, let us consider the equation $\alpha + \beta = \gamma^3$, with $\alpha, \beta \in \mathcal{O}_{S_K}^*$. By scaling the equation by triple powers of 3 and swapping α and β if necessary, we may assume $0 \leq v_{\mathfrak{P}}(\beta) \leq v_{\mathfrak{P}}(\alpha)$ with $v_{\mathfrak{P}}(\beta) \in \{0, 1, 2\}$. Also, we can assume that β is positive, otherwise we multiply everything by -1.
Case (1): Suppose $v_{\mathfrak{P}}(\beta) = 2$. If $v_{\mathfrak{P}}(\alpha) \geq 3$, then $v_{\mathfrak{P}}(\gamma^3) = v_{\mathfrak{P}}(\alpha + \beta) = 2$, which leads to a contradiction as $v_{\mathfrak{P}}(\gamma^3)$ must be a multiple of 3. Thus, $v_{\mathfrak{P}}(\alpha) = v_{\mathfrak{P}}(\beta) = 2$ and $v_{\mathfrak{P}}(\frac{\alpha}{\beta}) = 0 < 3$.
Case (2): Suppose $v_{\mathfrak{P}}(\beta) = 1$. If $v_{\mathfrak{P}}(\alpha) \geq 2$, then $v_{\mathfrak{P}}(\gamma^3) = v_{\mathfrak{P}}(\alpha + \beta) = 1$, which leads to a contradiction as $v_{\mathfrak{P}}(\gamma^3)$ must be a multiple of 3. Thus, $v_{\mathfrak{P}}(\alpha) = v_{\mathfrak{P}}(\beta) = 1$ and $v_{\mathfrak{P}}(\frac{\alpha}{\beta}) = 0 < 3$.
Case (3): Suppose $v_{\mathfrak{P}}(\beta) = 0$ with β not a cube. If $v_{\mathfrak{P}}(\alpha) > 3$, then $v_{\mathfrak{P}}(\gamma^3) = 0$ and $\beta \equiv \gamma^3 \mod 3^4$. Consider the field extension $L = K(\sqrt[3]{\beta}, \omega)$ of $K(\omega)$. We will show that L is unramified at 3, hence contradicting $3 \nmid h_{K(\omega)}$.

Consider the element $\delta := \frac{\gamma^2 + \gamma\omega\sqrt[3]{\beta} + \omega^2\sqrt[3]{\beta}}{3}$. Its minimal polynomial is

$$m_\delta(X) = X^3 + \gamma\frac{\gamma^3 - \beta}{3}X^2 - \gamma^2 X + \frac{(\gamma^3 - \beta)^2}{27}.$$

This belongs to $\mathcal{O}_K[X]$ and has discriminant

$$\Delta = -2\gamma^3\frac{(\gamma^3 - \beta)^3}{3^5} - 4\gamma^3\frac{(\gamma^3 - \beta)^5}{3^9} + \gamma^6\frac{(\gamma^3 - \beta)^2}{3^2} - 4\gamma^6 - \frac{(\gamma^3 - \beta)^4}{3^3}.$$

We can deduce that $\Delta \equiv -4\gamma^6 \mod 3$, proving that L is unramified at 3. Thus, we must have $v_{\mathfrak{P}}(\alpha) \leq 3$, giving $v_{\mathfrak{P}}(\frac{\alpha}{\beta}) = v_{\mathfrak{P}}(\alpha) \leq 3$.
Case (4): Suppose β is a cube. By dividing everything through β, we can assume that $\beta = 1$. Then by the hypothesis of the theorem, we get $v_{\mathfrak{P}}(\frac{\alpha}{\beta}) = v_{\mathfrak{P}}(\alpha) \leq 3$.
All of the possible four cases lead to $v_{\mathfrak{P}}(\frac{\alpha}{\beta}) \leq 3 = 3v_{\mathfrak{P}}(3)$, so we can conclude the proof by Theorem 9. □

4.6 Proof of Theorem 12

Proof. Note that $d \equiv 2 \mod 3$ gives that 3 is inert in the quadratic field $K = \mathbb{Q}(\sqrt{d})$, take $\mathfrak{P}$ to be the unique prime above 3 and denote $S_K = \{\mathfrak{P}\}$. By Theorem 11 it is enough to check that every solution $(\alpha, \gamma) \in \mathcal{O}_{S_K}^* \times \mathcal{O}_{S_K}$ with $v_{\mathfrak{P}}(\alpha) \geq 0$ to the equation $\alpha + 1 = \gamma^3$ satisfies $v_{\mathfrak{P}}(\alpha) \leq 3$.

Assume by a contradiction that we have a solution α to the above equation such that $v_{\mathfrak{P}}(\alpha) > 3$. This implies that $v_{\mathfrak{P}}(\gamma) = 0$, giving $\gamma \in \mathcal{O}_K$.
Rearranging we get that $(\gamma-1)(\gamma-\omega)(\gamma-\omega^2) = \alpha$ when viewed over $L := K(\omega)$. In the new field extension L we have that $(3)\mathcal{O}_L = (\omega-1)^2\mathcal{O}_L$. We take $\mathfrak{p} = (\omega-1)\mathcal{O}_L$ and $S_L = \{\mathfrak{p}\}$. Denote $x = \gamma - 1$ and $y = \gamma - \omega$, $z = \gamma - \omega^2$ and observe that

$$\begin{cases} x - y = (\omega - 1) \\ y - z = \omega(\omega - 1) \end{cases} \tag{17}$$

Note that $x, y, z \in \mathcal{O}_{S_L}$ and they are factors of the S_K-unit α, hence they must be S_L-units.

Consider $\tau \in \mathrm{Gal}(L/K)$ such that $\tau(\omega) = \omega^2$. It is easy to see that

$$\tau(x) = x, \quad \tau(y) = z \text{ and } \tau(\mathfrak{p}) = \mathfrak{p}.$$

This implies that $v_{\mathfrak{p}}(y) = v_{\mathfrak{p}}(z) =: r$. We will show that $r = 1$. Firstly note that by (17) we get that $1 = v_{\mathfrak{p}}(\omega(\omega-1)) = v_{\mathfrak{p}}(y - z) \geq r$. Suppose $r \leq 0$. Then $v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(xyz) = v_{\mathfrak{p}}(\alpha) \geq 8$ since $3^4 | \alpha$. Then, by using (17) again, we will get $1 = v_{\mathfrak{p}}(\omega - 1) = v_{\mathfrak{p}}(x - y) = r \leq 0$, a contradiction. So, r must be exactly 1. As $v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(xyz) = 8$, we must have $v_{\mathfrak{p}}(x) = 6$. Consider now

$$u := \frac{x}{\omega - 1} \text{ and } v = \frac{-y}{\omega - 1}.$$

By the above discussion, we will get that $\mathfrak{p}^5 | u$ and $v \in \mathcal{O}_L^*$. Denote $F := \mathbb{Q}(\omega)$. As v is a unit, we must have

$$\mathrm{Norm}_{L/F}(v) \in \mathcal{O}_F^* = \langle \omega + 1 \rangle \tag{18}$$

As $u + v = 1$, we get that $v \equiv 1 \mod 3$. Let σ be the generator of $\mathrm{Gal}(L/F)$. By noting that $3 | \sigma(u)$, we get that $\sigma(v) \equiv 1 \mod 3$ and consequently $\mathrm{Norm}_{L/F}(v) = v\sigma(v) \equiv 1 \mod 3$. This and (18) give $\mathrm{Norm}_{L/F}(v) = 1$. Suppose that $v \in \mathcal{O}_L^* \setminus \mathcal{O}_K^* = \omega\mathcal{O}_K^*$, then $\omega | \mathrm{Norm}_{L/F}(v)$ contradicting $\mathrm{Norm}_{L/F}(v) = 1$. Thus $v \in \mathcal{O}_K^*$ giving $u = 1 - v \in \mathcal{O}_K$ which is a contradiction as u is a ratio of a K-integer and $\omega - 1 \notin K$. □

4.7 Proof of Theorem 13

We first need to prove some preliminary lemmas. Throughout this section, K denotes a totally real field of degree n, $L := K(\omega)$ and $F := \mathbb{Q}(\omega)$. Moreover, K satisfies the conditions (i), (ii), (iii) and (iv) in the statement of Theorem 13. More precisely let q be the prime which totally ramifies in K. Note that $q \geq 5$ so it is inert in F. Denote $\tilde{\mathfrak{q}} := (q)\mathcal{O}_F$ and take $\mathfrak{q}$ to be the unique prime above q in L, so that $(q)\mathcal{O}_L = \mathfrak{q}^n\mathcal{O}_L$. Take $\mathfrak{P}$ to be the unique prime above 3 in K and denote $S_K = \{\mathfrak{P}\}$. In L we have that $(3)\mathcal{O}_L = (\omega-1)^2\mathcal{O}_L$. We take $\mathfrak{p} = (\omega-1)\mathcal{O}_L$ and $S_L = \{\mathfrak{p}\}$.

Lemma 37. *Let $\lambda \in \mathcal{O}_L$, then there exists $\beta \in \mathbb{Z}[\omega]$ such that $\lambda \equiv b \mod \mathfrak{q}$ and*

$$\mathrm{Norm}_{L/F}(\lambda) \equiv b^n \mod \tilde{\mathfrak{q}}. \tag{19}$$

Proof. Note that $\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L \cong \mathbb{F}_q(\omega) \cong \mathbb{Z}[\omega]/q\mathbb{Z}[\omega]$. Thus, there exists $b \in \mathbb{Z}[\omega]$ such that $\lambda \equiv b \mod \mathfrak{q}$. Let $\bar{L}$ be the normal closure of L. Take $\sigma \in \mathrm{Gal}(\bar{L}/F)$. Note that

$$(\sigma(\mathfrak{q}\mathcal{O}_{\bar{L}}))^n = \sigma(q\mathcal{O}_{\bar{L}}) = q\mathcal{O}_{\bar{L}} = (\mathfrak{q}\mathcal{O}_{\bar{L}})^n.$$

Thus, by the unique factorisation of ideals we get $\sigma(\mathfrak{q}\mathcal{O}_{\bar{L}}) = \mathfrak{q}\mathcal{O}_{\bar{L}}$. Moreover, by applying σ to $\lambda \equiv b \mod \mathfrak{q}$ we get that $\sigma(\lambda) \equiv b \mod \mathfrak{q}\mathcal{O}_{\bar{L}}$. Finally multiplying everything together

$$\mathrm{Norm}_{L/F}(\lambda) = \prod_{\sigma} \sigma(\lambda) \equiv b^n \mod \mathfrak{q}\mathcal{O}_{\bar{L}}.$$

As $\lambda \in \mathcal{O}_L$, it follows that $\mathrm{Norm}_{L/F}(\lambda) \in \mathcal{O}_F$. Also $b^n \in \mathcal{O}_F$. Thus, $\mathrm{Norm}_{L/F}(\lambda) - b^n \in \mathcal{O}_F \cap \mathfrak{q}\mathcal{O}_{\bar{L}} = \tilde{q}\mathcal{O}_F$. Hence (19) holds. □

Lemma 38. *Suppose $\lambda \in \mathcal{O}_L^*$ and (ii) holds, i.e. $\gcd(n, q^2-1) = 1$. Then $(\lambda \mod \mathfrak{q}) \in \langle \omega + 1 \rangle = \{\pm 1, \pm(\omega+1), \pm\omega\}$.*

Proof. Let $b \in \mathbb{Z}[\omega]$ with $\lambda \equiv b \mod \mathfrak{q}$ as in Lemma 37. This gives us $\mathrm{Norm}_{L/F}(\lambda) \equiv b^n \mod \tilde{\mathfrak{q}}$. However, as λ is a unit, we must have

$$\mathrm{Norm}_{L/F}(\lambda) \in \mathcal{O}_F^* = \langle \omega + 1 \rangle.$$

Putting these together we get that $b^n \equiv (\omega+1)^i \mod \tilde{\mathfrak{q}}$. On the other hand, $b \in \mathcal{O}_F$ and maps to a non-zero element of $\mathcal{O}_F/\tilde{\mathfrak{q}}\mathcal{O}_F \cong \mathbb{F}_{q^2}$ thus $b^{q^2-1} \equiv 1 \mod \tilde{\mathfrak{q}}$. The assumption $\gcd(n, q^2-1) = 1$ is equivalent to the existence of integers u, v so that $un + v(q^2-1) = 1$. It follows that

$$b = (b^n)^u (b^{q^2-1})^v \equiv (\omega+1)^{iu} \mod \tilde{\mathfrak{q}}.$$

Thus, $(\lambda \mod \mathfrak{q}) \in \langle \omega + 1 \rangle = \{\pm 1, \pm(\omega+1), \pm\omega\}$. □

Proof of Theorem 13. We will reduce the problem to a simpler one as described in Section 4.6. More precisely, by using Theorem 11 and then rewriting the equation into an S_K-unit equation, we get that it is enough to show that there are no solutions to

$$u + v = 1 \tag{20}$$

with $(u, v) \in \mathcal{O}_{S_L}^* \times \mathcal{O}_L^*$ such that $\mathfrak{p}^5 | u$. We will show the slightly stronger statement that there are no solutions to (20) such that $9|u$.
Note that by (20) it follows that $v \equiv 1 \mod 9$. Thus $\sigma(v) \equiv 1 \mod 9$ for all conjugates $\sigma(v)$ of v in $\mathrm{Gal}(\bar{L}/F)$, where $\bar{L}$ is the normal closure of L. Hence, $\mathrm{Norm}_{L/F}(v) \equiv 1 \mod 9$. As v is a unit, we get $\mathrm{Norm}_{L/F}(v) \in \mathcal{O}_F^* = \langle \omega + 1 \rangle$. Thus, the only possibility is

$$\mathrm{Norm}_{L/F}(v) = 1. \tag{21}$$

By Lemma 38 applied with $\lambda = v$ we get that

$$(v \mod \mathfrak{q}) \in \langle \omega + 1 \rangle = \{\pm 1, \pm(\omega+1), \pm\omega\}. \tag{22}$$

If $v \equiv 1 \mod \mathfrak{q}$, then $u = 1 - v \equiv 0 \mod \mathfrak{q}$, so $\mathfrak{q}|u$, but this is false as u is an S_L-unit and $\mathfrak{p}$ and $\mathfrak{q}$ are different primes.
Thus $(v \mod \mathfrak{q}) \in \{-1, \pm(\omega+1), \pm\omega\}$. Then

$$(\mathrm{Norm}_{L/F}(v) \mod \mathfrak{q}) \in \{(-1)^n, (\pm(\omega+1))^n, (\pm\omega)^n\}. \tag{23}$$

Since $\gcd(n, q^2-1) = 1$ and $q \geq 5$ is a prime, it follows in particular that $2 \nmid n$ and $3 \nmid n$. This observation along with (23) proves that $\mathrm{Norm}_{L/F}(v) \mod \mathfrak{q} \not\equiv 1$, contradicting (21).

□

5 S-unit equations and computability

Finally, we will describe how to algorithmically check the hypothesises in our two main Theorems 3 and 9 by studying how to compute solutions of certain (linear) *S-unit equations* over the 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 of K.

Theorem 39 (Siegel)**.** *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 $\mathcal{O}_S^*$.

Remark 40. Methods of effectively computing solutions to S-unit were pioneered by De Weger's famous thesis [32] for $K = \mathbb{Q}$. His method of lattice approximation reduction algorithms was later generalized for all number fields by others, see for example Smart's [28]. Moreover, an S-unit solver for $a = b = 1$ has been implemented in the free open-source mathematics software, Sage by A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, D. Roe, C. Vincent, M. West in [1].

We will now study two non-linear equations involving S-units which are going to play a crucial role in checking the hypothesis of our Theorems 3 and 9. Let K be a number field and S a finite set of prime ideals. Consider the equation

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

There is a natural scaling action of $\mathcal{O}_S^*$ on the solutions. We regard two solutions $(\alpha_1, \beta_1, \gamma_1) \sim_i (\alpha_2, \beta_2, \gamma_2)$ as equivalent if there is some $\epsilon \in \mathcal{O}_S^*$ such that $\alpha_2 = \epsilon^i \alpha_1$, $\beta_2 = \epsilon^i \beta_1$ and $\gamma_2 = \epsilon \gamma_1$.

Theorem 41. *Let K be a number field and S a finite set of prime ideals. Consider the equation*

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

For $i = 2, 3$, the equation has a finite number of solutions up to the equivalence relation $\sim_i$. Moreover, these are effectively computable.

Proof. Let $i = 2$ and $(\alpha, \beta, \gamma) \in \mathcal{O}_S^* \times \mathcal{O}_S^* \times \mathcal{O}_S$ a solution to $\alpha + \beta = \gamma^2$. By Dirichlet Unit Theorem $\mathcal{O}_S^*$ is finitely generated, and hence $\mathcal{O}_S^*/(\mathcal{O}_S^*)^2$ is finite. Fix a set of representatives $\beta_1, \beta_2, ..., \beta_l$. We may scale our solution so that $\beta \in \{\beta_1, \beta_2, ..., \beta_l\}$. Thus, there are finitely many choices of β (up to $\sim_2$ equivalence) and we fix one of them. We next show that for each such choice of β, there is a finite number of distinct α, and thus, a finite number of triples (α, β, γ) up to $\sim_2$ equivalence.

We rewrite the equation as

$$(\gamma + \sqrt{\beta})(\gamma - \sqrt{\beta}) = \alpha \text{ over } L. \tag{24}$$

where $L := K(\sqrt{\beta})$. Denote by $x := \gamma + \sqrt{\beta}, y := \gamma - \sqrt{\beta}$ and consider $S' := \{\mathfrak{P}_L \text{ prime of } L : \mathfrak{P}_L | \mathfrak{P}_K, \text{ for some } \mathfrak{P}_K \in S\}$. We claim that

$$\frac{1}{2\sqrt{\beta}} x - \frac{1}{2\sqrt{\beta}} y = 1$$

and x, y are both S'-units in L. By Theorem 39, we get finitely many x, y, and thus finitely many possibilities for $\alpha = xy$. Moreover, these are computable by Remark 40. The claim that x, y are S'-units follows by considering the valuation of the product in (24) at the primes of L outside the set S'. Then, we use the definition of S' and the fact that α is an S-unit in K.

For $i = 3$, the argument works in a similar manner. Fixing a representative β of the finite quotient $\mathcal{O}_S^*/(\mathcal{O}_S^*)^3$, we rewrite the equation as

$$(\gamma - \sqrt[3]{\beta})(\gamma - \omega \sqrt[3]{\beta})(\gamma - \omega^2 \sqrt[3]{\beta}) = \alpha \text{ over } L \tag{25}$$

where $L = K(\omega, \sqrt[3]{\beta})$ and $\beta \neq -1$. Denote by $x := \gamma - \sqrt[3]{\beta}, y := \gamma - \omega \sqrt[3]{\beta}$, $S' := \{\mathfrak{P}_L \text{ prime of } L : \mathfrak{P}_L | \mathfrak{P}_K, \text{for some } \mathfrak{P}_K \in S\}$.

We make the quick note that for $\beta = -1$ we take $x := \gamma + 1$, $y = \gamma + \omega$, $L := K(\omega)$ and the rest of the argument follows the same, so it is omitted.

As in the previous case, by examining the product in (25) we get that x, y are both S'-units in L and

$$\frac{1}{(\omega - 1)\sqrt[3]{\beta}} x - \frac{1}{(\omega - 1)\sqrt[3]{\beta}} y = 1.$$

Thus, by Theorem 39, Remark 40 and the observation that $\alpha = xy(y - \omega(\omega - 1)\sqrt[3]{\beta})$, we can conclude the proof.

□

Remark 42. In the hypotheses of Theorems 3 and 9 one needs to examine the local behaviour of $\frac{\alpha}{\beta}$ which, by the above theorem, can only take a finite, computable number of values.

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 *Number Theory, Volume II: Analytic and Modern Tools.*GTM 240, Springer, 2007.

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

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

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

[8] M. Derickx, F. Najman, S. Siksek. *Elliptic curves over totally real cubic field are modular.* Alg. Number Th. 14 (2020) 1791-1800.

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

[10] Nuno Freitas, Alain Kraus, and Samir Siksek. *Local criteria for the unit equation and the asymptotic Fermat's Last Theorem.* Proceedings of the National Academy of Sciences Mar 2021, 118 (12) e2026449118;

[11] 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.

[12] N. Freitas, S. Siksek. *The asymptotic Fermat's Last Theorem for five-sixths of real quadratic fields.* Compositio Mathematica, 151(8), 1395-1415.

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

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

[15] 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).

[16] E. Işik, y. Kara, e. Ozman. *On ternary Diophantine equations of signature* $(p, p, 2)$ *over number fields.* Turkish Journal of Mathematics, (2020) 44: 1197 – 1211.

[17] F. Lemmermeyer. *Class Field Towers,* 111 pages, September 7, 2010

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

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

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

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

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

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

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

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

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

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

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

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

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

[31] 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.

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

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

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

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