CLASS FIELD THEORY, DIOPHANTINE ANALYSIS AND THE ASYMPTOTIC FERMAT'S LAST THEOREM

NUNO FREITAS, ALAIN KRAUS, AND SAMIR SIKSEK

Abstract. Recent results of Freitas, Kraus, Şengün and Siksek, give sufficient criteria for the asymptotic Fermat's Last Theorem to hold over a specific number field. Those works in turn build on many deep theorems in arithmetic geometry. In this paper we combine the aforementioned results with techniques from class field theory, the theory of p-groups and p-extensions, Diophantine approximation and linear forms in logarithms, to establish the asymptotic Fermat's Last Theorem for many infinite families of number fields, and for thousands of number fields of small degree. For example, we prove the effective asymptotic Fermat's Last Theorem for the infinite family of fields $\mathbb{Q}(\zeta_{2^r})^+$ where $r \geq 2$.

1. Introduction

Let K be a number field, and let $\mathcal{O}_K$ be its ring of integers. The Fermat equation with prime exponent p over K is the equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K. \tag{1}$$

A solution (a, b, c) of (1) is called trivial if $abc = 0$, otherwise non-trivial. The celebrated Fermat's Last Theorem, proved by Wiles [31], asserts that the only solutions to (1) with $K = \mathbb{Q}$ and $p \geq 3$ are the trivial ones. The same statement, but for $p \geq 5$, was proved for $\mathbb{Q}(\sqrt{2})$ by Jarvis and Meekin [14], by Freitas and Siksek [10] for a handful of other real quadratic fields, and by Kraus [15] for the real cubic fields with discriminants 148, 404, 564, and the quartic field $\mathbb{Q}(\zeta_{16})^+$.

The equation (1) defines a curve of gonality $p - 1$, and one can use this to show that there are non-trivial solutions over infinitely many number fields of degree $\leq p - 1$. Therefore a sharp bound on p as in the works cited above does not exist for all number fields. This remains true even if we restrict ourselves to totally real number fields, as done for example in [9] and [15]. Indeed, the field $\mathbb{Q}^{\mathrm{tr}}$, obtained by taking the union of all totally real fields inside a given algebraic closure of $\mathbb{Q}$, is ample [21]. Thus for each fixed exponent p, the curve (1) has infinitely many points in $\mathbb{Q}^{\mathrm{tr}}$. It thus becomes natural to consider the question asymptotically.

The *asymptotic Fermat's Last Theorem over K* (or asymptotic FLT for short) is the statement that there is a bound B_K, depending only on the field K, such that for all prime exponents $p > B_K$, all solutions to (1) are trivial. If B_K is effectively

Date: October 2, 2019.

2010 *Mathematics Subject Classification.* Primary 11D41, Secondary 11R37, 11J86.

Key words and phrases. Fermat, modularity, class field theory, Diophantine analysis.

Freitas is supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 747808 and the grant *Proyecto RSME-FBBVA* 2015 *José Luis Rubio de Francia*. Siksek is supported by an *EPSRC LMF: L-Functions and Modular Forms Programme Grant EP/K034383/1*.

computable, we shall refer to this as the *effective asymptotic Fermat's Last Theorem over K*. Let ζ_3 be a primitive cube root of unity. The asymptotic FLT is false if $\zeta_3 \in K$ as $(1, \zeta_3, \zeta_3^2)$ is a solution to (1) for all $p \neq 3$. It seems reasonable to make the following conjecture which is a consequence of the *abc*-conjecture for number fields (see [4]).

Conjecture. *Let K be a number field. If $\zeta_3 \notin K$ then the asymptotic Fermat's Last Theorem holds for K.*

In [9], Freitas and Siksek give a criterion for asymptotic FLT for totally real K. This criterion can be formulated in terms of the solutions of a certain S-unit equation, where S is the set of primes of K above 2, or equivalently in terms of elliptic curves defined over K having full 2-torsion, good reduction away from S and with specified behaviour at the primes in S. The proof builds on many deep results, including modularity lifting theorems over totally real fields due to Kisin, Gee and others, Merel's uniform boundedness theorem, and Faltings' theorem for rational points on curves of genus ≥ 2. In [22], Şengün and Siksek establish a similar criterion for asymptotic FLT for a general number field K, subject to two standard conjectures. In this paper we build on these results, and with the help of class field theory, the theory of p-groups and p-extensions, Diophantine approximation and linear forms in logarithms, we establish asymptotic FLT for many infinite families of number fields, and for thousands of number fields of small degree. We remark that class field theory, and theory of cyclotomic fields, was once considered the key to Fermat's Last Theorem [16]. That approach was dramatically surpassed by the ideas of Frey, Serre, Ribet and Wiles. This paper demonstrates that class field theory still has a rôle to play in the beautiful story of Fermat.

A Conjecture of Kraus. This paper is inspired by the following conjecture.

Conjecture (Kraus [15])**.** *Let K be a totally real number field with narrow class number 1. Suppose 2 is totally ramified in K and write $\mathfrak{P}$ for the unique prime above 2. Then there are no elliptic curves over K with full 2-torsion and conductor $\mathfrak{P}$.*

Kraus showed that his conjecture implies asymptotic FLT for such K. One objective of this paper is to prove Kraus' conjecture in the following strengthened form.

Theorem 1. *Let ℓ be a rational prime. Let K be a number field satisfying the following conditions:*

(i) $\mathbb{Q}(\zeta_\ell) \subseteq K$, *where ζ_ℓ is a primitive ℓ-th root of unity;*
(ii) *K has a unique prime λ above ℓ;*
(iii) $\gcd(h_K^+, \ell(\ell-1)) = 1$ *where h_K^+ is the narrow class number of K.*

Then there is no elliptic curve E/K with a K-rational ℓ-isogeny, good reduction away from λ and potentially multiplicative reduction at λ.

The proof can be found in Section 3, and makes use of class field theory, and the theory of p-groups and p-extensions.

Asymptotic FLT for some infinite families of number fields. The second objective of this paper is to use Theorem 1 to prove asymptotic FLT for several infinite families of number fields. Our results will be unconditional for totally real fields. For number fields K having at least one complex embedding, our theorems

are conditional on two standard conjectures. We postpone the precise statements of the two conjectures till Section 4, and now only briefly mention what they are.

- Conjecture 4.1: this is a weak version of Serre's modularity conjecture over general number fields.
- Conjecture 4.2: this is a conjecture in the Langlands Programme which says that every weight 2 newform over K with rational integer Hecke eigenvalues has an associated elliptic curve over K or a fake elliptic curve over K.

Before stating our main results, we need to introduce some notation. For a number field K, we denote the class group by $\mathrm{Cl}(K)$ and the narrow class group by $\mathrm{Cl}^+(K)$. Their orders are respectively the class number h_K, and the narrow class number h_K^+. The class number h_K is the degree of the Hilbert class field, which is the largest abelian everywhere unramified extension of K. The narrow class number h_K^+ is the degree of the narrow class field, which is the largest abelian extension of K unramified at all the finite places. We shall write $h_{K,2}^+$ for the largest power of 2 dividing h_K^+. This the degree of the narrow Hilbert 2-class field of K, which is the largest abelian 2-extension of K unramified at all the finite places. The degree $h_{K,2}^+$ is of course also the order of the 2-Sylow subgroup of $\mathrm{Cl}^+(K)$. For an ideal $\mathfrak{P}$ of $\mathcal{O}_K$ we denote its class in $\mathrm{Cl}^+(K)$ by $[\mathfrak{P}]$.

Theorem 2. *Let K be a number field satisfying the following two hypotheses:*

(a) *2 is totally ramified in K;*
(b) *$h_{K,2}^+$ divides the order of $[\mathfrak{P}]$ in $\mathrm{Cl}^+(K)$, where $\mathfrak{P}$ is the unique prime above 2.*

Then the following hold.

(i) *If K is totally real, then the asymptotic FLT holds over K. Moreover, if all elliptic curves over K with full 2-torsion are modular, then the effective asymptotic FLT holds over K.*
(ii) *If K has at least one complex embedding, and we assume Conjectures 4.1 and 4.2 over K then the asymptotic FLT holds over K.*

We can substantially strengthen the conclusion by adding one more assumption to the theorem. By a 2-extension K' of K we mean a Galois extension of K whose degree is a power of 2.

Theorem 3. *Let K be a number field satisfying the following three hypotheses:*

(a) *2 is totally ramified in K;*
(b) *$h_{K,2}^+$ divides the order of $[\mathfrak{P}]$ in $\mathrm{Cl}^+(K)$, where $\mathfrak{P}$ is the unique prime above 2;*
(c) *h_K is odd.*

Let K'/K be any 2-extension unramified away from $\mathfrak{P}$ (and in particular unramified at the infinite places).

(i) *If K' is totally real, then the asymptotic FLT holds over K'. Moreover, if all elliptic curves over K' with full 2-torsion are modular, then the effective asymptotic FLT holds over K'.*
(ii) *If K' has at least one complex embedding, and we assume Conjectures 4.1 and 4.2 over K' then the asymptotic FLT holds over K'.*

We immediately obtain the following easy consequence of Theorem 3.

Corollary 1.1. *Let K be a totally real number field where 2 is totally ramified. Suppose that h_K^+ is odd. Then asymptotic FLT holds over any totally real 2-extension of K unramified away from 2.*

Proof. Clearly, if the narrow class number h_K^+ is odd, then $h_K = h_K^+$ and $h_{K,2}^+ = 1$ and so hypotheses (b), (c) are automatically satisfied. Hypothesis (a) is satisfied by assumption. □

Let $r \geq 2$, and let ζ_{2^r} be a primitive 2^r-th root of unity. Write $\mathbb{Q}(\zeta_{2^r})^+$ for the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$. We now give a few consequences of Theorem 3.

Corollary 1.2. *Let K be a totally real number field satisfying (a), (b), (c). Write K_r for the compositum $K \cdot \mathbb{Q}(\zeta_{2^r})^+$. Then the asymptotic FLT holds for K_r.*

We note that the family $\{K_r\}$ are the layers in the $\mathbb{Z}_2$-cyclotomic extension of K. Of course $K = \mathbb{Q}$ does satisfy (a), (b), (c). Here we can be more precise.

Corollary 1.3. *The effective asymptotic Fermat's Last Theorem holds over $\mathbb{Q}(\zeta_{2^r})^+$.*

Proof. For effectivity, we observe that $\mathbb{Q}(\zeta_{2^r})^+$ is contained in the $\mathbb{Z}_2$-extension of $\mathbb{Q}$, and that modularity of elliptic curves over $\mathbb{Z}_p$-extensions of $\mathbb{Q}$ has been established by Thorne [28]. □

Note that $K = \mathbb{Q}(\zeta_{2^r})^+$ is respectively $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$ for $r = 2, 3$. In these cases Corollary 1.3 is known in the stronger (non-asymptotic) form and is due respectively to Wiles [31] and to Jarvis and Meekin [14], as previously mentioned. For $r = 4$ and 5, it is proved by Kraus [15, Théorème 9] with $B_K = 3$ and $B_K = 6724$ respectively.

Corollary 1.4. *Let $K/\mathbb{Q}$ be a 2-extension unramified away from 2 and ∞. If K has at least one complex embedding, assume Conjectures 4.1 and 4.2 over K. Then the asymptotic FLT holds for K.*

Proof. The fact that such K satisfies conditions (a), (b) is a result of Markšaĭtis [19] (we do however reprove this as Corollary 2.4). □

Corollary 1.5. *Let K be a real quadratic field. Then K satisfies conditions (a), (b), (c) of Theorem 3 if and only if $K = \mathbb{Q}(\sqrt{2})$ or $K = \mathbb{Q}(\sqrt{\ell})$ or $K = \mathbb{Q}(\sqrt{2\ell})$ for some prime $\ell \equiv 3 \pmod 8$. In particular, for such K, the asymptotic FLT holds over $K_r = K \cdot \mathbb{Q}(\zeta_{2^r})^+$ for all $r \geq 2$.*

The proof of this corollary is given in Section 7. We remark in passing that the only imaginary quadratic fields that satisfy conditions (a), (b), (c) are $K = \mathbb{Q}(i)$ and $K = \mathbb{Q}(\sqrt{-2})$, as we explain in Section 7. Applying Theorem 2 to these two fields will merely give special cases of Corollary 1.4, however the stronger form of FLT over these fields has already been established by Turcas [29], subject only to Conjecture 4.1.

After the quadratic case, we establish asymptotic FLT for a very explicit infinite family of totally real cubic fields. This is done in Section 8.

Theorem 4. *Let K be a totally real cubic field satisfying the following three conditions:*

(i) *2 is either totally ramified or inert in K;*
(ii) *3 ramifies in K;*

(iii) *the discriminant Δ_K is non-square (i.e. the Galois group of the normal closure of K is S_3).*

Then the asymptotic Fermat's Last Theorem holds for K.

Corollary 1.6. *There is a positive proportion of totally cubic real fields (ordered by discriminant) satisfying asymptotic FLT.*

Proof. This now follows from [2, Theorem 8] and [8]. □

The previous series of results establish asymptotic FLT over infinitely many number fields. It is natural to wonder if we can establish asymptotic FLT over some number field of every possible degree. We are able to give an affirmative though conditional answer.

Theorem 5. *Let $n \geq 2$ be an integer. There are infinitely many number fields of degree n for which the asymptotic FLT holds subject to Conjectures 4.1 and 4.2.*

Moreover, if $n = 2^k$ with $k \geq 1$ or $n = 3$ then there are infinitely many totally real fields of degree n for which asymptotic FLT holds (unconditionally).

Proof. For the second statement we take the fields K_r in Corollary 1.5 for varying ℓ, plus Corollary 1.6. Thus we suppose $n \geq 5$. By Theorem 2 all we need to do is show that there are infinitely many number fields of degree n such that 2 is totally ramified and having odd narrow class number. For this we need a special case of a remarkable theorem of Ho, Shankar and Varma [12, Theorem 4]. Let $M/\mathbb{Q}_2$ be any totally ramified extension of degree n; for example $M = \mathbb{Q}_2(\sqrt[n]{2})$. Let $r_2 \geq 1$, and $r_1 = n - 2r_2$. The theorem of Ho, Shankar and Varma asserts the existence of infinitely many number fields K of degree n, signature (r_1, r_2), and odd narrow class number, satisfying that $K \otimes \mathbb{Q}_2 = M$.

□

A Computational Criterion for Asymptotic FLT. The third objective of this paper is to provide a computationally viable criterion for establishing asymptotic FLT over specific number fields. The papers [9] and [22] give computational criteria for asymptotic FLT in terms of the solutions of a certain S-unit equation. There are algorithms for determining the solutions to S-unit equations (e.g. [25, Chapter IX]). However these algorithms require knowledge of the full unit group $\mathcal{O}_K^\times$ of the number field K. Provably determining the full unit group seems to be a computationally hard problem, and is impractical in current implementations (e.g. `Magma` [3], `Pari/GP` [20]) if the degree is much larger than 20. It is however much easier to determine a subgroup V (say) of the unit group $\mathcal{O}_K^\times$ of full rank ([5], [7], [11]). Moreover, once one has a subgroup V of full rank, it is easy [1, Section 5.3] for any given prime p to p-saturate V, i.e. to replace V by a larger subgroup of $\mathcal{O}_K^\times$ whose index is coprime to p. The following theorem gives a criterion for asymptotic FLT that assumes knowledge not of the full unit group but only of a subgroup of full rank that is 2-saturated.

Theorem 6. *Let K be a number field with one prime $\mathfrak{P}$ above 2. Let V be a subgroup of $\mathcal{O}_K^\times$ such that the index $[\mathcal{O}_K^\times : V]$ is finite and odd. Let*

$$U := \{u \in V \,:\, u \equiv 1 \pmod{16\mathfrak{P}}\}.$$

Suppose every element of U is the square of a unit. Then the following hold.

(A) *There is no elliptic curve E/K with full 2-torsion and conductor $\mathfrak{P}$.*

(B) *If K is totally real and 2 is totally ramified in K then the asymptotic FLT holds over K.*
(C) *Suppose K is a number field over which Conjectures 4.1 and 4.2 hold, and 2 is totally ramified in K. Then the asymptotic FLT holds over K.*

Theorem 6 is proved in Section 6. We remark that the criterion of the theorem is easy to test computationally. One simply computes U as the kernel of the natural map $V \to (\mathcal{O}_K/16\mathfrak{P})^\times$, and then tests whether each element in a chosen generating set is a square. As an illustration, let

$$f_n(x) = \frac{1}{2\sqrt{-7}}\left((1+\sqrt{-7})(x+\sqrt{-7})^n - (1-\sqrt{-7})(x-\sqrt{-7})^n\right), \qquad n \geq 1 \tag{2}$$

The polynomial f_n is monic, belongs to $\mathbb{Z}[x]$, and defines a number field $K_n = \mathbb{Q}[x]/f_n(x)$ that is totally real and in which 2 totally ramifies (Lemma 10.1). Our computational criterion establishes asymptotic Fermat over K_n for $1 \leq n \leq 6$, $8 \leq n \leq 14$, $15 \leq n \leq 20$, $23 \leq n \leq 27$, $n = 29, 31, 32$. This and other examples are found in Section 10, where we also compare the relative strength of Theorems 2 and 6, both computationally and theoretically.

Diophantine analysis and asymptotic FLT. Whilst class field theory has distinguished historical connections to Fermat's Last Theorem, the subject of Diophantine analysis (Diophantine approximation, linear forms in logarithms) seems to have had little or no influence on the mathematics of the Fermat equation. In a surprising twist, recent works ([9], [22]) give criteria for asymptotic FLT over certain number fields conditional on properties of the solutions of a specific S-unit equation. Whilst the S-unit equation is treated by ad hoc methods in [9], [22], and by class field theory for much of this paper, the principal method of studying S-unit equations is through Diophantine analysis (e.g. [25]). The final objective of this paper is to demonstrate that the methods of Diophantine analysis can be useful in attacking asymptotic FLT over number fields.

Theorem 7. *Let $\ell \equiv 1 \pmod{24}$ be a prime. The asymptotic FLT holds over $\mathbb{Q}(\sqrt{\ell})$.*

The proof is given in Sections 11–12. We remark that the family of quadratic fields treated in this theorem is disjoint from those treated in [9] or in the previous parts of this paper. Indeed, in the family treated in Theorem 7, the prime 2 splits, whereas both in [9] and in earlier parts of this paper, the focus is on number fields with exactly one prime above 2. That assumption is essential for the arguments of [9], and appears essential to the class field theoretic arguments of this paper.

Acknowledgements. We would like to thank Alex Bartel, Dominique Bernardi, Luis Dieulefait, Hendrik Lenstra, Bjorn Poonen, David Roberts and Haluk Şengün for useful discussions.

2. p-GROUPS AND p-EXTENSIONS

Let p be a prime. A finite group G is said to be a p-group if its order $\#G$ is a power of p. A finite extension of fields L/K is a p-extension if it is Galois and its degree $[L : K]$ is a power of p. Of course the Galois group $\mathrm{Gal}(L/K)$ of a p-extension L/K is a p-group. In this section we collect well-known facts about p-groups and p-extensions that we will make use of later.

The following is a standard result concerning p-groups; see for example [26, Section 2.1].

Lemma 2.1. *Let G be a p-group. Then every maximal subgroup of G is normal of index p.*

We will denote the Frattini subgroup of a finite group G by $\Phi = \Phi(G)$; this is defined as the intersection of all maximal subgroups of G. The following is known as the *Burnside basis theorem* [26, Theorem 2.1.16].

Theorem 8. *Let G be a p-group. Then $G/\Phi(G) \cong (\mathbb{Z}/p\mathbb{Z})^r$ for some r, and so can be considered as an r-dimensional $\mathbb{F}_p$-vector space. Let $x_1, \dots, x_s \in G$ and write $y_i = x_i\Phi(G) \in G/\Phi(G)$. Then $G = \langle x_1, \dots, x_s \rangle$ if and only if $y_1, \dots, y_s$ span $G/\Phi(G)$. In particular, G can be generated by r elements.*

Corollary 2.2. *Let G be a p-group, and write G' for its derived subgroup. Suppose G/G' is cyclic. Then G is cyclic and $G' = 1$.*

Proof. By Theorem 8 we know that $G/\Phi(G)$ is abelian, and thus $\Phi(G) \supseteq G'$. We therefore have a natural surjection $G/G' \to G/\Phi(G)$. It follows that $G/\Phi(G)$ is cyclic. By Burnside's Basis Theorem G is cyclic. □

Finally we shall need the following standard result from Galois theory for which we are unable to find a convenient reference.

Lemma 2.3. *Let L/K and M/L be p-extensions. Let N/K be the Galois closure of M/K. Then N/K is a p-extension.*

Proof. Write $G = \mathrm{Gal}(N/K)$, $H = \mathrm{Gal}(N/L)$, $I = \mathrm{Gal}(N/M)$. By the Galois correspondence and the hypotheses we have

$$I \trianglelefteq H \trianglelefteq G,$$

where the quotients G/H and H/I are p-groups. We are required to show that G is a p-group. Since $\#G = \#H \cdot \#\,\mathrm{Gal}(L/K)$ it is sufficient to show that H is a p-group.

For $\sigma \in G$, we note that $\mathrm{Gal}(N/M^\sigma) = \sigma I \sigma^{-1}$. Observe, as H is normal in G, that $\sigma I \sigma^{-1} \trianglelefteq H$ and the quotient $H/\sigma I \sigma^{-1}$ is isomorphic to H/I, and so is a p-group. As N/K is the Galois closure of M/K, we know that N is generated by the fields M^σ, and so $\cap \sigma I \sigma^{-1} = 1$. Therefore the natural map

$$H \to \prod_{\sigma \in G} H/\sigma I \sigma^{-1}$$

is an injection. As the group on the right is a p-group, H is also a p-group. □

Let K be a number field. Recall that the Hilbert class field is the largest abelian everywhere unramified extension of K; its degree is the class number, which we denote by h_K. The narrow Hilbert class field of K is the maximal abelian extension of K unramified away from the infinite places; its degree is the narrow Hilbert class number which we denote by h_K^+.

We would like to thank Hendrik Lenstra for drawing our attention to the following result. Part (a) is a result of Iwasawa [13] (a proof is also found in [30, Theorem 10.4]). Part (b) is a straightforward generalization.

Theorem 9. *Let K be a number field and let $\mathfrak{q}$ be a finite prime of K.*

(a) *Suppose $p \nmid h_K$. Let K'/K be a p-extension unramified away from $\mathfrak{q}$ (and in particular, unramified at the infinite places). Then $\mathfrak{q}$ is totally ramified in K' and $p \nmid h_{K'}$.*

(b) *Suppose $p \nmid h_K^+$. Let K'/K be a p-extension unramified away from $\mathfrak{q}$ and the infinite places. Then $\mathfrak{q}$ is totally ramified in K' and $p \nmid h_{K'}^+$.*

Proof. We prove (b). The proof of (a) is almost identical. Write $G = \mathrm{Gal}(K'/K)$. Let $\mathfrak{q}'$ be a prime of K' above K. Let I denote the inertia subgroup of G for $\mathfrak{q}'/\mathfrak{q}$. To show that $\mathfrak{q}$ is totally ramified in K' is enough to show that $I = G$. Suppose I is a proper subgroup of G. By Lemma 2.1 there is a normal index p subgroup H of G containing I. Consider $K'' = K'^H \subset K'$. This is a Galois degree p extension of K. As H contains I, the extension K''/K is unramified at some prime $\mathfrak{q}''$ above $\mathfrak{q}$ (and below $\mathfrak{q}'$). But K''/K is Galois, and so it is unramified at all the primes above $\mathfrak{q}$. It follows that K''/K is a cyclic degree p extension unramified away from the infinite places, contradicting $p \nmid h_K^+$. Therefore $\mathfrak{q}$ is totally ramified in K'.

To complete the proof we would like to show that $p \nmid h_{K'}^+$. Suppose otherwise. So there is a cyclic degree p extension L/K' unramified away from the infinite places. Now let M/K be the Galois closure of L/K. This is a p-extension by Lemma 2.3, and it is unramified away from $\mathfrak{q}$ and the infinite places. It follows from the first part that $\mathfrak{q}$ is totally ramified in M/K. However, $M \supseteq L \supsetneq K' \supseteq K$ and L/K' is unramified at any prime above $\mathfrak{q}$ giving a contradiction. □

The following is a result of Markšaĭtis [19]. It is immediate from part (b) of Theorem 9.

Corollary 2.4. *Let $K/\mathbb{Q}$ be a 2-extension unramified away from 2, ∞. Then K has odd narrow class number and 2 totally ramifies in K.*

3. Proof of Theorem 1

Let ℓ be a rational prime. Let K be a number field satisfying conditions (i)–(iii) of Theorem 1. In particular, there is a unique prime λ of K above ℓ. Let $G_K = \mathrm{Gal}(\overline{K}/K)$ be and $I_\lambda \subset G_K$ an inertia subgroup at λ.

Before we prove the theorem, let us highlight the core idea. We will work by contradiction, so suppose there is an elliptic curve E/K that is a counterexample to the theorem. We show the existence of a quadratic twist F/K such that the ℓ-adic Galois representation $\rho_{F,\ell} : G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ attached to F satisfies

$$\rho_{F,\ell}(G_K) = \rho_{F,\ell}(I_\lambda);$$

that is, the global image of $\rho_{F,\ell}$ is equal to the image of a local Galois group. In general, a global image is huge whilst a local image is much smaller, so this situation is prone to a contradiction, which we will show to happen in our setting.

We now prove the theorem. Suppose there is an elliptic curve E/K having a K-rational ℓ-isogeny, good reduction away from λ, and potentially multiplicative reduction at λ.

Claim: there is a quadratic twist F/K of E of conductor λ such that $K(F[\ell^n])/K$ is an ℓ-extension for all $n \geq 1$.

We first show how this claim implies the theorem. Indeed, by the criterion of Néron–Ogg–Shafarevich [24, Proposition IV.10.3], the extension $K(F[\ell^n])/K$ is unramified away from λ and the infinite places. By assumption (iii), we have $\ell \nmid h_K^+$, hence part (b) of Theorem 9 to deduce that λ is totally ramified in $K(F[\ell^n])/K$. Let $n \geq 1$ and consider

$$\overline{\rho}_{F,\ell^n} : G_K \to \mathrm{GL}(F[\ell^n]) \cong \mathrm{GL}(\mathbb{Z}/\ell^n\mathbb{Z})$$

the mod ℓ^n representation of F. The Galois group of the extension $K(F[\ell^n])/K$ is $\overline{\rho}_{F,\ell^n}(G_K)$ and its inertia subgroup at λ is $\overline{\rho}_{F,\ell^n}(I_\lambda)$. As the extension is totally ramified, we have

$$\overline{\rho}_{F,\ell^n}(G_K) = \overline{\rho}_{F,\ell^n}(I_\lambda).$$

However, the latter group is reducible by the theory of the Tate curve (see [24, Exercise V.5.13]). As F does not have complex multiplication (it has a multiplicative prime) this contradicts Serre's open image theorem [23, Chapter IV] for sufficiently large n. (Note that taking the limit on n leads to the equality of ℓ-adic representations as in the discussion above.)

It remains to establish our claim. The curve E has potentially multiplicative reduction at λ, and the theory of the Tate curve (c.f. [24, Exercises V.5.11 and V.5.13]) gives a precise description of the restriction of the representation $\overline{\rho}_{E,\ell}$ to the decomposition group D_λ:

$$\overline{\rho}_{E,\ell}|_{D_\lambda} \sim \begin{pmatrix} \eta \cdot \chi_\ell & * \\ 0 & \eta \end{pmatrix} \tag{3}$$

where χ_ℓ is the modulo ℓ cyclotomic character, and η is a character of D_λ which is trivial or quadratic. Moreover, the (local) twist $E \otimes \eta$ is an elliptic curve defined over K_λ having split multiplicative reduction at λ.

As E has a K-rational ℓ-isogeny, the mod ℓ representation is reducible:

$$\overline{\rho}_{E,\ell} \sim \begin{pmatrix} \phi & * \\ 0 & \psi \end{pmatrix}$$

where ϕ, ψ are characters $G_K \to \mathbb{F}_\ell^*$. It follows from the criterion of Néron–Ogg–Shafarevich that ϕ and ψ are unramified except possibly at λ and the infinite places. By assumption (i), the mod ℓ cyclotomic character is trivial on G_K. From (3) we have $\phi|_{I_\lambda} = \psi|_{I_\lambda} = \eta|_{I_\lambda}$ is of order dividing 2. Thus ϕ/ψ and ϕ^2 are characters of G_K of order dividing $\ell - 1$ that are unramified away from the infinite places. By assumption (iii), the narrow class number h_K^+ is coprime to $\ell - 1$, thus $\phi/\psi = \phi^2 = 1$. Hence $\phi = \psi$ is a quadratic character of G_K. We let F be the (global) quadratic twist $E \otimes \phi$. Now F/K has conductor λ, and

$$\overline{\rho}_{F,\ell} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Thus $\#\overline{\rho}_{F,\ell}(G_K) = 1$ or ℓ, hence $\overline{\rho}_{F,\ell}(G_K)$ is an ℓ-group. To complete the proof of our claim we need to show that $\overline{\rho}_{F,\ell^n}(G_K)$ is an ℓ-group for all n. Consider the commutative diagram

$$\begin{array}{ccc} G_K & \xrightarrow{\overline{\rho}_{F,\ell^n}} & \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \\ & \searrow^{\overline{\rho}_{F,\ell}} & \downarrow \pi \\ & & \mathrm{GL}_2(\mathbb{F}_\ell) \end{array}$$

where π is the reduction modulo ℓ map. From this we deduce the exact sequence

$$1 \to \overline{\rho}_{F,\ell^n}(G_K) \cap \ker(\pi) \to \overline{\rho}_{F,\ell^n}(G_K) \to \overline{\rho}_{F,\ell}(G_K) \to 1.$$

We know already that $\overline{\rho}_{F,\ell}(G_K)$ is an ℓ-group. Thus it is sufficient to show that $\ker(\pi)$ is an ℓ-group. However,

$$\ker(\pi) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,:\, a,\ b,\ c,\ d \in \mathbb{Z}/\ell^n\mathbb{Z}, \quad a \equiv d \equiv 1,\ b \equiv c \equiv 0 \pmod{\ell} \right\}.$$

We see that $\#\ker(\pi) = \ell^{4n-4}$, proving our claim, and completing the proof. □

4. Criteria for Asymptotic FLT

Freitas and Siksek [9] give a criterion for the asymptotic FLT over a totally real field K in terms of solutions to a certain S-unit equation. Şengün and Siksek [22] give similar criterion for general number fields, assuming standard conjectures that we state below. In this section we state these results, and then show that they can be sharpened for number fields where 2 is totally ramified.

The S-unit equation. Let K be a number field. Let

$$\begin{gathered} S = \{\mathfrak{P} \,:\, \mathfrak{P} \text{ is a prime of } K \text{ above } 2\}, \\ T = \{\mathfrak{P} \in S \,:\, f(\mathfrak{P}/2) = 1\}, \qquad U = \{\mathfrak{P} \in S \,:\, 3 \nmid \mathrm{ord}_{\mathfrak{P}}(2)\}. \end{gathered} \tag{4}$$

Here $f(\mathfrak{P}/2)$ denotes the residual degree of $\mathfrak{P}$. The ring of S-integers is

$$\mathcal{O}_S = \{\alpha \in K \,:\, \mathrm{ord}_{\mathfrak{q}}(\alpha) \geq 0 \text{ for all primes } \mathfrak{q} \notin S\}.$$

We let $\mathcal{O}_S^\times$ be the unit group of $\mathcal{O}_S$; explicitly

$$\mathcal{O}_S^\times = \{\alpha \in K \,:\, \mathrm{ord}_{\mathfrak{q}}(\alpha) = 0 \text{ for all primes } \mathfrak{q} \notin S\}.$$

Consider the S-unit equation

$$\lambda + \mu = 1, \qquad \lambda,\ \mu \in \mathcal{O}_S^\times, \tag{5}$$

and let $\mathfrak{S}_3$ be the subgroup of $\mathrm{PGL}_2(K)$ given by

$$\mathfrak{S}_3 = \{\, z,\ 1/z,\ 1-z,\ 1/(1-z),\ z/(z-1),\ (z-1)/z\}.$$

As explained in [9, Section 6], there is an action of $\mathfrak{S}_3$ on the solutions to (5) given by $\sigma(\lambda,\mu) = (\sigma(\lambda), 1-\sigma(\lambda))$ for $\sigma \in \mathfrak{S}_3$. The solutions $(2,-1)$, $(-1,2)$, $(1/2,1/2)$ form an orbit under the action of $\mathfrak{S}_3$ that we call the *irrelevant orbit*. Other solutions are called *relevant*.

A criterion of asymptotic FLT over totally real fields. The following is (a special case of) Theorem 3 of [9].

Theorem 10. *Let K be a totally real field and let S, T and U be as* (4)*. Suppose that either $T \neq \varnothing$ or $[K:\mathbb{Q}]$ is odd. Suppose that for every solution (λ,μ) to the S-unit equation* (5) *there is*

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

Then the asymptotic FLT holds over K.

A criterion of asymptotic FLT over general fields. For now K will be a general number field—by general we simply mean that we do not require it to be totally real. We will soon state a theorem of Şengün and Siksek [22] which gives a criterion for asymptotic FLT over general number fields. This criterion is dependent on two standard conjectures which we now state in precise form. However we do not apply the conjectures directly, and so we omit any further discussion of them; instead we recommend the exposition of these conjectures in [22, Sections 2–4] as well the references cited therein. The first conjecture is a special case of Serre's modularity conjecture over K.

Conjecture 4.1. *Let $\overline{\rho} : G_K \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be an odd, irreducible, continuous representation with Serre conductor $\mathcal{N}$ (prime-to-p part of its Artin conductor) and such that $\det(\overline{\rho}) = \chi_p$ is the mod p cyclotomic character. Assume that p is unramified in K and that $\overline{\rho}|_{G_{K_\mathfrak{p}}}$ arises from a finite-flat group scheme over $\mathcal{O}_\mathfrak{p}$ for every prime $\mathfrak{p} \mid p$. Then there is a (weight 2) mod p eigenform θ over K of level $\mathcal{N}$ such that for all primes $\mathfrak{q}$ coprime to $p\mathcal{N}$, we have*

$$\mathrm{Tr}(\overline{\rho}(\mathrm{Frob}_\mathfrak{q})) = \theta(T_\mathfrak{q}),$$

where $T_\mathfrak{q}$ denotes the Hecke operator at $\mathfrak{q}$.

We point out that the condition $\det(\overline{\rho}) = \chi_p$ is inadvertently omitted in [22].

The second conjecture is in essence a generalization of the Eichler–Shimura theorem for rational weight 2 eigenforms.

Conjecture 4.2. *Let $\mathfrak{f}$ be a (weight 2) complex eigenform over K of level $\mathcal{N}$ that is non-trivial and new. If K has some real place, then there exists an elliptic curve $E_\mathfrak{f}/K$, of conductor $\mathcal{N}$, such that*

$$\#E_\mathfrak{f}(\mathcal{O}_K/\mathfrak{q}) = 1 + \mathbf{N}\mathfrak{q} - \mathfrak{f}(T_\mathfrak{q}) \quad \text{for all } \mathfrak{q} \nmid \mathcal{N}. \tag{6}$$

If K is totally complex, then there exists either an elliptic curve $E_\mathfrak{f}$ of conductor $\mathcal{N}$ satisfying (6) or a fake elliptic curve $A_\mathfrak{f}/K$, of conductor $\mathcal{N}^2$, such that

$$\#A_\mathfrak{f}(\mathcal{O}/\mathfrak{q}) = \left(1 + \mathbf{N}\mathfrak{q} - \mathfrak{f}(T_\mathfrak{q})\right)^2 \quad \text{for all } \mathfrak{q} \nmid \mathcal{N}.$$

The following is Theorem 1.1 of [22].

Theorem 11. *Let K be a number field over which Conjectures 4.1 and 4.2 hold. Let S, T be as in (4). Suppose $T \neq \varnothing$. Suppose that for every solution (λ, μ) to the S-unit equation (5) there is some $\mathfrak{P} \in T$ that satisfies $\max\{|\mathrm{ord}_\mathfrak{P}(\lambda)|, |\mathrm{ord}_\mathfrak{P}(\mu)|\} \leq 4\,\mathrm{ord}_\mathfrak{P}(2)$. Then the asymptotic FLT holds over K.*

A simplification when $\#S = 1$. The following proposition is a simplification and strengthening of the ideas in [9, Section 6], under the additional hypothesis that the set S has precisely one element. It allows us to simplify the condition on the S-unit equation in Theorems 10 and 11. The proof makes use of ideas found in the proof of [15, Lemme 1].

Proposition 4.3. *Let K be a number field with precisely one prime $\mathfrak{P}$ above 2, and let $S = \{\mathfrak{P}\}$. The following are equivalent.*

(i) *There is an elliptic curve E/K with full 2-torsion and conductor $\mathfrak{P}$.*
(ii) *There is an elliptic curve E/K with full 2-torsion, potentially good reduction away from $\mathfrak{P}$, and potentially good multiplicative reduction at $\mathfrak{P}$.*

(iii) *There is a solution* (λ,μ) *to the* S*-unit equation* (5) *with* $\mathrm{ord}_{\mathfrak{P}}(\mu)=0$ *and* $\mathrm{ord}_{\mathfrak{P}}(\lambda)>4\,\mathrm{ord}_{\mathfrak{P}}(2)$.

(iv) *There is a solution* (λ,μ) *to the* S*-unit equation* (5) *with*

$$\max\{|\mathrm{ord}_{\mathfrak{P}}(\lambda)|,|\mathrm{ord}_{\mathfrak{P}}(\mu)|\}>4\,\mathrm{ord}_{\mathfrak{P}}(2).$$

Proof. Clearly (iii) implies (iv). If we have a solution as in (iv), we simply observe that we can produce a solution satisfying (iii) by applying a suitable element of $\mathfrak{S}_3$. This proves the equivalence of (iii) and (iv). Clearly (i) implies (ii). To complete the proof it is enough to show that (ii) implies (iii) and that (iii) implies (i).

We suppose (ii). The elliptic curve E has the form

$$E\,:\,Y^2=X(X-a)(X+b)$$

with $a,\,b\in K$ and $ab(a+b)\neq 0$. Let $c=-a-b$. Then $a+b+c=0$. Applying a permutation to a, b, c allows us to suppose that $\mathrm{ord}_{\mathfrak{P}}(b)\geq\mathrm{ord}_{\mathfrak{P}}(c)\geq\mathrm{ord}_{\mathfrak{P}}(a)$. If this permutation is cyclic then the resulting elliptic curve is isomorphic to our original model, and if non-cyclic then it is a quadratic twist by -1.

Let $\lambda=-b/a$, $\mu=-c/a$. Then,

$$\lambda+\mu=1,\qquad \mathrm{ord}_{\mathfrak{P}}(\lambda)\geq\mathrm{ord}_{\mathfrak{P}}(\mu)\geq 0. \tag{7}$$

The quadratic twist of E by $-a$ is

$$E'\,:\,Y^2=X(X+1)(X+\lambda). \tag{8}$$

and also has potentially multiplicative reduction at $\mathfrak{P}$ and potentially good reduction away from $\mathfrak{P}$. In the usual notation, the invariants of E' are

$$c_4=16(\lambda^2-\lambda+1),\qquad c_6=-64(1-\lambda/2)(1-2\lambda)(1+\lambda)$$
$$\Delta=16\lambda^2(\lambda-1)^2,\qquad j=\frac{2^8(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}.$$

If $\mathfrak{q}$ is a prime $\nmid 2$ then $\mathrm{ord}_{\mathfrak{q}}(j)\geq 0$, and we easily check from the above formulae that this forces $\mathrm{ord}_{\mathfrak{q}}(\lambda)=\mathrm{ord}_{\mathfrak{q}}(\mu)=\mathrm{ord}_{\mathfrak{q}}(\Delta)=0$. If $\mathrm{ord}_{\mathfrak{P}}(\lambda)=0$ then, by (7), $\mathrm{ord}_{\mathfrak{P}}(1-\lambda)=0$ and so $\mathrm{ord}_{\mathfrak{P}}(j)>0$ giving a contradiction. Thus $\mathrm{ord}_{\mathfrak{P}}(\lambda)=t$ with $t>0$, and as $\mu=1-\lambda$, we have $\mathrm{ord}_{\mathfrak{P}}(\mu)=0$. Since $\mathrm{ord}_{\mathfrak{P}}(j)=8\cdot\mathrm{ord}_{\mathfrak{P}}(2)-2t<0$ we have $\mathrm{ord}_{\mathfrak{P}}(\lambda)=t>4\,\mathrm{ord}_{\mathfrak{P}}(2)$. This proves that (ii) implies (iii).

We now suppose (λ,μ) are as in (iii). We let E' be the elliptic curve given by (8). This model is integral and has good reduction at all $\mathfrak{q}\nmid 2$. As $\mathrm{ord}_{\mathfrak{P}}(\lambda)>4\,\mathrm{ord}_{\mathfrak{P}}(2)$, Hensel's Lemma shows that the expressions $\lambda^2-\lambda+1$, $1-\lambda/2$, $1-2\lambda$ and $1+\lambda$ are all $\mathfrak{P}$-adic squares. Thus $-c_4/c_6$ is an $\mathfrak{P}$-adic square. By [24, Theorem V.5.3] the elliptic curve E' has split multiplicative reduction at $\mathfrak{P}$. This shows that (iii) implies (i). □

Theorem 12. *Let* K *be a number field. If* K *has complex embeddings, assume Conjectures 4.1 and 4.2. Suppose* 2 *is totally ramified in* K *and let* $\mathfrak{P}$ *be the prime above* 2*. Suppose there is no elliptic curve* E/K *with full* 2*-torsion and conductor* $\mathfrak{P}$*. Then the asymptotic FLT holds over* K*.*

Proof. Here $S=T=\{\mathfrak{P}\}$. By Proposition 4.3, as there is no elliptic curve with full 2-torsion and conductor $\mathfrak{P}$, every solution to (5) satisfies $\max\{|\mathrm{ord}_{\mathfrak{P}}(\lambda)|,|\mathrm{ord}_{\mathfrak{P}}(\mu)|\}\leq 4\,\mathrm{ord}_{\mathfrak{P}}(2)$. The theorem follows from Theorem 10 if K is totally real, and from Theorem 11 otherwise. □

5. Proof of Theorem 2

Let K be a number field. The narrow Hilbert p-class field of K is the maximal abelian p-extension of K unramified away from the finite places. This is a subextension of the narrow Hilbert class field of degree $p^{\mathrm{ord}_p(h_K^+)}$. We thank D. Bernardi for suggesting the proof of the following lemma.

Lemma 5.1. *Let K be a number field and L the narrow Hilbert p-class field of K. Suppose $\mathrm{Gal}(L/K)$ is cyclic. Then $p \nmid h_L^+$.*

Proof. Let M be the narrow Hilbert p-class field of L. To establish the lemma we merely have to show that $M = L$. First we claim that M/K is Galois. To see this suppose that $\sigma \in \mathrm{Gal}(\overline{K}/K)$ where we identify L, M as subfields of $\overline{K}$. Now L/K is Galois and so $L^\sigma = L$. Thus M and M^σ are both the unique maximal abelian p-extension of $L = L^\sigma$ unramified at all finite places, and so must be equal. It follows that M/K is Galois. We remark that M/K is a p-extension (Lemma 2.3) unramified at all finite places.

Let $G = \mathrm{Gal}(M/K)$ and let G' its derived subgroup. As $\mathrm{Gal}(L/K) \cong G/\mathrm{Gal}(M/L)$ is abelian, the subgroup $\mathrm{Gal}(M/L)$ contains G'. Thus the fixed field $M^{G'}$ satisfies $L \subset M^{G'} \subset M$. However $\mathrm{Gal}(M^{G'}/K) \cong G/G'$ which is abelian; thus $M^{G'}$ is an abelian p-extension of K unramified at the finite places and so is contained in L. It follows that $M^{G'} = L$. Hence $\mathrm{Gal}(M/L) \cong G'$ and $G/G' \cong \mathrm{Gal}(L/K)$ which is cyclic. From Corollary 2.2, the derived group $G' \cong \mathrm{Gal}(M/L)$ is trivial, and so $M = L$ as required. □

Proposition 5.2. *Let K is a number field with exactly one prime $\mathfrak{P}$ above 2. Let L be the narrow Hilbert 2-class field of K. The following are equivalent.*

(i) *There exists a finite extension M/K with unique prime above 2 and odd narrow class number.*
(ii) *L has unique prime above 2.*
(iii) *L has a unique prime above 2 and odd narrow class number.*
(iv) *The order of $[\mathfrak{P}]$ in $\mathrm{Cl}^+(K)$ is divisible by $h_{K,2}^+$.*

Proof. Suppose (i) is satisfied. Then LM is a 2-extension of M unramified away from the infinite places. Thus $LM = M$, and so $L \subseteq M$. In particular, L has a unique prime above 2. Thus (ii) is satisfied.

Now suppose (ii) is satisfied. As $\mathfrak{P}$ is unramified in L, and there is a unique prime above $\mathfrak{P}$, we see that $\mathfrak{P}$ is inert in L. Thus $\mathrm{Gal}(L/K)$ is equal to the decomposition group at $\mathfrak{P}$ which is cyclic. By Lemma 5.1 we know that L has odd narrow class number and so (iii) is satisfied. Clearly, (iii) implies both (i) and (ii) so we have now proved the equivalence of (i), (ii), (iii).

We complete the proof by showing that (ii) and (iv) are equivalent. Let N be the narrow class field of K. We consider the Artin map for the extension N/K. This is an isomorphism $\theta : \mathrm{Cl}^+(K) \to \mathrm{Gal}(N/K)$, sending $[\mathfrak{P}]$ to the Frobenius element $\mathrm{Frob}_{N/K,\mathfrak{P}}$. We compose this with the natural restriction map $\phi : \mathrm{Gal}(N/K) \twoheadrightarrow \mathrm{Gal}(L/K)$. Let H be the 2-Sylow subgroup of $\mathrm{Gal}(N/K)$, and H' be the maximal subgroup of odd order. As $\mathrm{Gal}(N/K)$ is abelian, $\mathrm{Gal}(N/K) = H \oplus H'$. Recall that $\#\mathrm{Gal}(L/K) = h_{K,2}^+ = \#H$. Thus the restriction $\phi|_H : H \to \mathrm{Gal}(L/K)$ is an isomorphism. The map ϕ sends $\mathrm{Frob}_{N/K,\mathfrak{P}}$ to $\mathrm{Frob}_{L/K,\mathfrak{P}}$. Note that L has a unique prime above 2 if and only if $\mathrm{Frob}_{L/K,\mathfrak{P}}$ has order $\#\mathrm{Gal}(L/K) = h_{K,2}^+$. This

is equivalent to $\mathrm{Frob}_{N/K,\mathfrak{P}}$ having order divisible by $h^+_{K,2}$, which is equivalent to $[\mathfrak{P}]$ having order divisible by $h^+_{K,2}$. □

Corollary 5.3. *Let K is a number field with exactly one prime $\mathfrak{P}$ above 2. Suppose that the order $[\mathfrak{P}]$ in $\mathrm{Cl}^+(K)$ is divisible by $h^+_{K,2}$. Then there is no elliptic curve E/K with a K-point of order 2, good reduction away from $\mathfrak{P}$, and potentially multiplicative reduction at $\mathfrak{P}$.*

Proof. Let L be the narrow 2-class field of K. By Proposition 5.2 the number field L has one prime λ above 2 and odd narrow class number. Suppose there is an elliptic curve E/K as in the statement. Recall that good reduction and potentially multiplicative reduction are preserved by base change. Therefore, the curve E/L has an L-point of order 2, good reduction away from λ, and potentially multiplicative reduction at λ. Now Theorem 1 applied over L with $\ell = 2$ gives a contradiction. □

5.1. **Proof of Theorem 2.** Theorem 2 follows immediately from Theorem 12 together with Corollary 5.3.

6. Proof of Theorem 3

In this section K, $\mathfrak{P}$ satisfy assumptions (a), (b), (c) of Theorem 3. Moreover, K'/K is a 2-extension that is unramified away from $\mathfrak{P}$ (and in particular, unramified at the infinite places). By the first part of Theorem 9, the prime $\mathfrak{P}$ is totally ramified in K', and thus 2 is totally ramified in K'. We stress that it is here that we have made use of the fact that h_K is odd (assumption (c)). We denote by $\mathfrak{P}'$ the unique prime of K' above 2.

Next we let L be the narrow 2-class field of K. As assumptions (a), (b) are satisfied, Proposition 5.2 tells that h^+_L is odd, and L has unique prime $\mathfrak{q}$ (say) above 2. Let $L' = LK'$. As K'/K is a 2-extension unramified away from $\mathfrak{P}$, the extension L'/L is a 2-extension unramified away from $\mathfrak{q}$. Now we apply the second part of Theorem 9 to the extension L'/L to deduce that $h^+_{L'}$ is odd, and that there is a unique prime $\mathfrak{q}'$ say above $\mathfrak{q}$ (and so $\mathfrak{q}'$ is the unique prime of L' above 2). In particular, by Theorem 1, there is no elliptic curve E/L' with an L'-rational point of order 2 and conductor $\mathfrak{q}'$. As $L' \supseteq K'$, it follows (as in the proof of Corollary 5.3) that there is no elliptic curve E/K' with K'-rational point of order 2 and conductor $\mathfrak{P}'$.

The proof is completed by applying Theorem 12 with K' and $\mathfrak{P}'$ instead of K and $\mathfrak{P}$. □

Example. We give an example to illustrate the importance of assumption (c) for proof of Theorem 3. Let $K = \mathbb{Q}(\alpha)$ be the totally real quartic field with α satisfying $\alpha^4 - 10\alpha^2 - 8\alpha + 7 = 0$. Then 2 totally ramifies in K and we denote the prime above 2 by $\mathfrak{P}$. We checked using the computer algebra package `Magma` that $\mathrm{Cl}^+(K)$ is cyclic of order 4 generated by $[\mathfrak{P}]$. Thus asymptotic FLT holds for K by Theorem 2.

However $h_K = 2$, and so condition (c) is not satisfied. The Hilbert class field of K is in fact the quadratic extension $K(\sqrt{2}) = K \cdot \mathbb{Q}(\zeta_8)^+$. Of course $\mathfrak{P}$ is not ramified in this extension, and so by Proposition 5.2 it is inert. It follows that the unique prime $\mathfrak{P}_r$ above 2 in $K_r = K \cdot \mathbb{Q}(\zeta_{2^r})^+$ has residue field $\mathbb{F}_4$ for all r. We are therefore unable to apply Theorem 12 (with K_r in place of K). By [9, Theorem 3] if there is an non-trivial solution to the Fermat equation over K_r with p suitably large, and we allow ourselves to assume a suitable Eichler–Shimura conjecture, then

there is an elliptic curve F/K_r with full 2-torsion and good reduction away from $\mathfrak{P}_r$. However, this result does not specify potentially multiplicative reduction at $\mathfrak{P}_r$ when the residue field is not $\mathbb{F}_2$.

7. Proof of Corollary 1.5

In this section K is a quadratic field (real or imaginary). We want to understand when K satisfies conditions (a), (b), (c) of Theorem 3. We start by recalling some basic facts from genus theory, following [17, Section 1.3.1]. Let D be the discriminant of K. The **prime discriminants** are the integers -4, 8, -8, and $(-1)^{(\ell-1)/2}\ell$, where ℓ is an odd prime. The discriminant D can be written as a product $D = d_1 d_2 \cdots d_t$ where the d_j are prime discriminants, and this factorization is unique up to reordering. The 2-ranks of the class group and the narrow class group of K have convenient expressions in terms of this factorization:

$$(9)\quad \dim_{\mathbb{F}_2} \mathrm{Cl}^+(K)[2] = t-1, \quad \dim_{\mathbb{F}_2} \mathrm{Cl}(K)[2] = \begin{cases} t-1 & \text{if } D<0 \\ t-1 & \text{if all } d_j>0, \\ t-2 & \text{if } D>0 \text{ and some } d_j<0. \end{cases}$$

For the remainder of this section we assume that 2 ramifies in K, i.e. condition (a). After reordering the d_j if necessary, we have $d_1 = -4$, 8 or -8. The following is immediate from (9).

Lemma 7.1. *h_K^+ is odd if and only if $K = \mathbb{Q}(i)$, $K = \mathbb{Q}(\sqrt{2})$ or $K = \mathbb{Q}(\sqrt{-2})$.*

Lemma 7.2. *h_K is odd and h_K^+ is even if and only if $K = \mathbb{Q}(\sqrt{\ell})$ or $K = \mathbb{Q}(\sqrt{2\ell})$ where $\ell \equiv 3 \pmod 4$ is a prime. In this case the 2-Sylow subgroup of $\mathrm{Cl}^+(K)$ has order 2.*

Proof. From (9) we see that h_K is odd and h_K^+ is even if and only if $t = 2$, $d_1 < 0$, and $d_2 < 0$. In particular, $d_1 = -4, -8$. Recall that the discriminant D of a quadratic field $\mathbb{Q}(\sqrt{d})$ (d square-free) is d if $d \equiv 1 \pmod 4$ and $4d$ otherwise. From this it is easy to deduce the first part of the lemma.

It then follows in this case that $\mathrm{Cl}^+(K)[2] \cong \mathbb{Z}/2\mathbb{Z}$. Write $\mathrm{Cl}^+(K)[2^\infty]$ for the 2-Sylow subgroup of $\mathrm{Cl}^+(K)$. For the second part of the lemma we want to show that $\mathrm{Cl}^+(K)[2^\infty] = \mathrm{Cl}^+(K)[2]$. This can easily be deduced from a standard exact sequence [6, Proposition 3.2.3] relating the class group and narrow class group. Alternatively, let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$ representing a class $[\mathfrak{a}]$ in $\mathrm{Cl}^+(K)[2^\infty]$; we would like to show that $[\mathfrak{a}] \in \mathrm{Cl}^+(K)[2]$. As h_K is odd, $\mathfrak{a}^r = \alpha \cdot \mathcal{O}_K$ for some non-zero $\alpha \in \mathcal{O}_K$ with r odd. Then $\mathfrak{a}^{2r} = \alpha^2 \mathcal{O}_K$ and α^2 is totally positive, and so $[\mathfrak{a}]^{2r} = 1$ in $\mathrm{Cl}^+(K)$. As r is odd, $[\mathfrak{a}] \in \mathrm{Cl}^+(K)[2]$. □

Application of Theorem 3 to Quadratic Fields. We shall prove Corollary 1.5. The second part of the corollary follows from the first part and Theorem 3 as the fields K_r are totally real 2-extensions of K.

We now prove the first part. For this we would like to know all real quadratic fields satisfying conditions (a), (b), (c) in the statement of Theorem 3. By Lemmas 7.1 and 7.2 we see these are the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{d})$ where $d = \ell$ or $d = 2\ell$ and $\ell \equiv 3 \pmod 4$ is a prime. Moreover, from the second part of Lemma 7.2, we see that to prove the corollary it is enough to show that $[\mathfrak{P}]$ generates $\mathrm{Cl}^+(K)[2^\infty] = \mathrm{Cl}^+(K)[2] \cong \mathbb{Z}/2\mathbb{Z}$ if and only if $\ell \equiv 3 \pmod 8$. As 2 ramifies in K, we have $\mathfrak{P}^2 = 2\mathcal{O}_K$. Thus $[\mathfrak{P}]$ has order 1 or 2 in $\mathrm{Cl}^+(K)$ and it is precisely

in the latter case that $[\mathfrak{P}]$ generates $\mathrm{Cl}^+(K)[2]$. However the class number is odd, so $\mathfrak{P}$ must be principal. We may write $\mathfrak{P} = \beta\mathcal{O}_K$, with $\beta = a + b\sqrt{d} > 0$ where a, $b \in \mathbb{Z}$. Since $\ell \equiv 3 \pmod 4$, quadratic reciprocity implies the norm of any unit is 1, and so every unit is totally positive or totally negative. Our positive generator β for $\mathfrak{P}$ is therefore unique up to multiplication by a totally positive unit. Thus $[\mathfrak{P}]$ has order 2 in $\mathrm{Cl}^+(K)$ if and only if $\overline{\beta} < 0$, where $\overline{\beta} = a - b\sqrt{d}$. However,

$$\beta \cdot \overline{\beta} = a^2 - db^2 = 2 \cdot \eta, \qquad \eta = \pm 1.$$

Thus $[\mathfrak{P}]$ has order 2 in $\mathrm{Cl}^+(K)$ if and only if $\eta = -1$. Now $\ell \mid d$, and so $2 \cdot \eta$ is a quadratic residue modulo ℓ. We deduce that $\eta = -1$ if and only if $\ell \equiv 3 \pmod 8$ completing the proof.

8. Proof of Theorem 4

In this section K is a totally real cubic field with 2 either totally ramified or inert, 3 ramified, and Δ_K (the discriminant) a non-square. We would like to show that K satisfies asymptotic FLT. For this we will apply Theorem 10. Write $\mathfrak{P}$ for the unique prime above 2. In the notation of that theorem (c.f. (4)), we have

$$\begin{cases} S = T = \{\mathfrak{P}\},\ U = \varnothing & \textbf{case (I)}\text{: if 2 is totally ramified in } K, \\ S = U = \{\mathfrak{P}\},\ T = \varnothing & \textbf{case (II)}\text{: if 2 inert in } K. \end{cases}$$

We shall show that conditions (A), (B) of Theorem 10 respectively hold for all solutions (λ, μ) to the S-unit equation (5) according to whether we are in case (I) or (II). Note that the action of $\mathfrak{S}_3$ on (λ, μ) preserves the value $\max\{|\mathrm{ord}_{\mathfrak{P}}(\lambda)|, |\mathrm{ord}_{\mathfrak{P}}(\mu)|\}$, and also the residue class of $\mathrm{ord}_{\mathfrak{P}}(\lambda\mu)$ modulo 3. Thus need only show that conditions (A), (B) hold for a representative of each $\mathfrak{S}_3$-orbit. Now for a solution (λ, μ) we may apply a suitable element of $\mathfrak{S}_3$ so that

$$\mathrm{ord}_{\mathfrak{P}}(\lambda) = m \geq 0, \qquad \mathrm{ord}_{\mathfrak{P}}(\mu) = 0.$$

Write

$$\mathrm{Norm}(\lambda) = \eta_1 \cdot 2^n, \qquad \mathrm{Norm}(\mu) = \eta_2, \qquad \eta_1 = \pm 1,\ \eta_2 = \pm 1, \quad n = \begin{cases} m & \text{case (I)} \\ 3m & \text{case (II)}. \end{cases}$$

If $\mu \in \mathbb{Q}$, then μ is a unit in $\mathbb{Z}$ and so $\mu = \pm 1$ which gives $(\lambda, \mu) = (2, -1)$ which satisfies (A), (B) respectively for cases (I), (II). We therefore suppose $\mu \notin \mathbb{Q}$ and so $K = \mathbb{Q}(\mu)$. The minimal polynomial of μ has the form

$$f(X) = X^3 + aX^2 + bX - \eta_2,$$

for some a, $b \in \mathbb{Z}$. Write Δ_f for the discriminant of f. Then

$$\Delta_f = [\mathcal{O}_K : \mathbb{Z}[\mu]]^2 \cdot \Delta_K.$$

Recall that $3 \mid \Delta_K$ and Δ_K is not a square. Therefore $3 \mid \Delta_f$ and Δ_f is not a square.

Note that the minimal polynomial for $\lambda = 1 - \mu$ is $-f(1 - X)$ as $\lambda \notin \mathbb{Q}$; therefore its constant coefficient must be $-\mathrm{Norm}(\lambda)$. We deduce

$$b = \eta_1 \cdot 2^n - 1 + \eta_2 - a, \qquad f = X^3 + aX^2 + (\eta_1 \cdot 2^n - 1 + \eta_2 - a)X - \eta_2.$$

The discriminant Δ_f is now an expression that depends on only a, n, η_1, η_2; we denote this by $\Delta(a, n, \eta_1, \eta_2)$. Let $a_0 \in \{0, 1, 2\}$, $n_0 \in \{0, 1\}$ satisfy $a \equiv a_0 \pmod 3$, $n \equiv n_0 \pmod 2$. Note that $2^n \equiv 2^{n_0} \pmod 3$. Thus

$$\Delta(a_0, n_0, \eta_1, \eta_2) \equiv \Delta(a, n, \eta_1, \eta_2) = \Delta_f \equiv 0 \pmod 3.$$

We computed $\Delta(a_0, n_0, \eta_1, \eta_2)$ for the 24 possible $(a_0, n_0, \eta_1, \eta_2)$ with $a_0 \in \{0, 1, 2\}$, $n_0 \in \{0, 1\}$ and $\eta_1, \eta_2 \in \{1, -1\}$. We found $\Delta(a_0, n_0, \eta_1, \eta_2) \equiv 0 \pmod 3$ for precisely the following two possibilities

$$(a_0, n_0, \eta_1, \eta_2) = (0, 0, -1, -1) \quad \text{or} \quad (0, 1, 1, -1). \tag{10}$$

In particular $\eta_2 = -1$.

Case (I). We will show condition (A) of Theorem 10 holds, that is $m \le 12$. In fact we prove the stronger $m \le 5$. Thus we suppose $m \ge 6$. In particular $\mu = 1 - \lambda \equiv 1 \pmod{4\mathcal{O}_K}$ and so $-1 = \eta_2 = \mathrm{Norm}(\mu) \equiv 1 \pmod 4$ giving a contradiction.

Case (II). In this case $\mathfrak{P} = 2\mathcal{O}_K$. Thus $\mu = 1 - \lambda \equiv 1 \pmod{2^m\mathcal{O}_K}$, and so $-1 = \eta_2 = \mathrm{Norm}(\mu) \equiv 1 \pmod{2^m}$. Thus $m = 0$ or 1. If $m = 1$ then (B) is satisfied. So suppose $m = 0$, and so $n = 0$, and thus $n_0 = 0$. From (10) we deduce $\eta_1 = -1$. Hence

$$f = X^3 + aX^2 - (a + 3)X + 1.$$

We find that

$$\Delta_f = (a^2 + 3a + 9)^2.$$

This contradicts the fact that Δ_f is not a square, and completes the proof of Theorem 4.

9. Proof of Theorem 6

We merely have to prove (A). Parts (B), (C) follow from (A) and Theorem 12. Before proving (A) we will take a closer look at U. We suppose U, V satisfy the hypotheses of the theorem: the index $[\mathcal{O}_K^\times : V]$ is finite and odd, and every element of U is a square. Let

$$W := \{w \in \mathcal{O}_K^\times \ : \ w \equiv 1 \pmod{16\mathfrak{P}}\}.$$

Then U is contained in W and we claim that the index $[W : U]$ is finite and odd. Indeed, W is the kernel of the natural map $\mathcal{O}_K^\times \to (\mathcal{O}_K/16\mathfrak{P})^\times$, and U is the kernel of the restriction of this map to V. Consider the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U & \longrightarrow & V & \longrightarrow & (\mathcal{O}_K/16\mathfrak{P})^\times & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & W & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & (\mathcal{O}_K/16\mathfrak{P})^\times & \longrightarrow & 1 \end{array}$$

The snake lemma immediately gives $W/U \cong \mathcal{O}_K^\times/V$, and thus the index $[W : U]$ is finite and odd.

Next we show that every element of W is a square. Let $(\mathcal{O}_K^\times)^2$ be the subgroup of squares in $\mathcal{O}_K^\times$. The assumption that every element in U is a square is equivalent to saying that U is contained in $(\mathcal{O}_K^\times)^2$. As the index $[\mathcal{O}_K^\times : (\mathcal{O}_K^\times)^2]$ is a power of 2, and the index $[W : U]$ is odd, we see that W is also contained in $(\mathcal{O}_K^\times)^2$. We have now established our claim that every element of W is a square.

We turn to the proof of (A). Suppose (A) is false. By Proposition 4.3 there is a solution (λ, μ) to the S-unit equation satisfying

$$\mathrm{ord}_{\mathfrak{P}}(\mu) = 0, \qquad \mathrm{ord}_{\mathfrak{P}}(\lambda) > 4\,\mathrm{ord}_{\mathfrak{P}}(2). \tag{11}$$

As there are only finitely many solutions to the S-unit equation, we may suppose that (λ, μ) satisfies (11) with the value of $\mathrm{ord}_{\mathfrak{P}}(\lambda)$ as large as possible. Observe that $\mu \in \mathcal{O}_K^\times$. Moreover, $\mu = 1 - \lambda$ and so $\mu \equiv 1 \pmod{16\mathfrak{P}}$. Thus $\mu \in W$. It follows that $\mu = \varepsilon^2$ for some $\varepsilon \in \mathcal{O}_K^\times$. We may therefore rewrite (5) as $(1+\varepsilon)(1-\varepsilon) = \lambda$. Hence

$$1 + \varepsilon = \lambda_1, \qquad 1 - \varepsilon = \lambda_2, \qquad \lambda_1\lambda_2 = \lambda. \tag{12}$$

Here λ_1, λ_2 are in $\mathcal{O}_K \cap \mathcal{O}_S^\times$. Moreover, by interchanging $-\varepsilon$ with ε if necessary, we may suppose that

$$\mathrm{ord}_{\mathfrak{P}}(\lambda_1) \geq \mathrm{ord}_{\mathfrak{P}}(\lambda_2).$$

However $\mathrm{ord}_{\mathfrak{P}}(\lambda_1) + \mathrm{ord}_{\mathfrak{P}}(\lambda_2) = \mathrm{ord}_{\mathfrak{P}}(\lambda) > 4\,\mathrm{ord}_{\mathfrak{P}}(2)$. Thus $\mathrm{ord}_{\mathfrak{P}}(\lambda_1) > 2\,\mathrm{ord}_{\mathfrak{P}}(2)$. Now from (12) we have

$$2 = \lambda_1 + \lambda_2, \qquad 2\varepsilon = \lambda_1 - \lambda_2. \tag{13}$$

We immediately deduce that

$$\mathrm{ord}_{\mathfrak{P}}(\lambda_2) = \mathrm{ord}_{\mathfrak{P}}(2), \qquad \mathrm{ord}_{\mathfrak{P}}(\lambda_1) = \mathrm{ord}_{\mathfrak{P}}(\lambda) - \mathrm{ord}_{\mathfrak{P}}(\lambda_2) = \mathrm{ord}_{\mathfrak{P}}(\lambda) - \mathrm{ord}_{\mathfrak{P}}(2).$$

Multiplying the equations in (13) and rearranging we have

$$\lambda' + \mu' = 1, \qquad \lambda' := \frac{\lambda_1^2}{\lambda_2^2}, \quad \mu' := \frac{-4\varepsilon}{\lambda_2^2}.$$

Here we have a new solution (λ', μ') to the S-unit equation (5). Moreover,

$$\mathrm{ord}_{\mathfrak{P}}(\mu') = 0, \qquad \mathrm{ord}_{\mathfrak{P}}(\lambda') = 2\,\mathrm{ord}_{\mathfrak{P}}(\lambda) - 4\,\mathrm{ord}_{\mathfrak{P}}(2) > \mathrm{ord}_{\mathfrak{P}}(\lambda),$$

where the last inequality follows from (11). This contradicts the maximality of $\mathrm{ord}_{\mathfrak{P}}(\lambda)$ and completes the proof.

10. Examples and Comparisons

We wrote a short `Magma` implementation of the criterion of Theorem 6. We would of course like to compare this criterion with the criterion of Theorem 2. For $n \geq 3$ let $\mathcal{F}_n$ be the set of totally real fields of degree n, discriminant $\leq 10^6$, in which 2 totally ramifies. By the theorem of Odlyzko (quoted in [27, Proposition 2.3]),

$$29.009^n \cdot \exp(-8.3185) < 10^6.$$

It follows that $3 \leq n \leq 6$. We were able to find the complete sets $\mathcal{F}_3$, $\mathcal{F}_4$, $\mathcal{F}_5$, $\mathcal{F}_6$ in the John Jones `Number Field Database` [18]. It turns out that $\mathcal{F}_6$ is empty, so we focus on degree 3, 4, 5. We define the following sets.

- Let $\mathcal{G}_n$ be the set of $K \in \mathcal{F}_n$ such that h_K^+ is odd.
- Let $\mathcal{H}_n$ be the set of $K \in \mathcal{F}_n$ such that $[\mathfrak{P}] \in \mathrm{Cl}^+(K)$ has order divisible by $h_{K,2}^+$ and h_K is odd.
- Let $\mathcal{I}_n$ be the set of $K \in \mathcal{F}_n$ such that $[\mathfrak{P}] \in \mathrm{Cl}^+(K)$ has order divisible by $h_{K,2}^+$.
- Let $\mathcal{J}_n$ be the set of $K \in \mathcal{F}_n$ such that every element of U is a square (where we take $V = \mathcal{O}_K^\times$).

Of course $\mathcal{G}_n \subseteq \mathcal{H}_n \subseteq \mathcal{I}_n$. We know the asymptotic FLT holds for any K belonging to $\mathcal{I}_n$ or $\mathcal{J}_n$, thanks to Theorems 2 and 6. We computed these sets using our `Magma` implementation. The results are summarised in the table.

n	$\#\mathcal{F}_n$	$\#\mathcal{G}_n$	$\#\mathcal{H}_n$	$\#\mathcal{I}_n$	$\#\mathcal{J}_n$
3	8600	3488	3488	3488	7653
4	1243	1	428	446	1039
5	23	13	13	13	22

We make the following observations.

(I) As 2 is totally ramified in all these fields, $2\mathcal{O}_K = \mathfrak{P}^n$. If $n = 3, 5$, then the order of $[\mathfrak{P}]$ in $\mathrm{Cl}^+(K)$ is odd. It follows that $\mathcal{G}_n = \mathcal{H}_n = \mathcal{I}_n$.

(II) For $n = 3, 4, 5$, we found that $\mathcal{I}_n \subset \mathcal{J}_n$. An explanation for this is given by Lemma 10.2 below.

(III) Note that $\#\mathcal{G}_4 = 1$. In other words, there is only one totally real quartic field K of discriminant $\leq 10^6$ for which h_K^+ is odd. This field is $K = \mathbb{Q}(\zeta_{16})^+$. This observation is explained by Theorem 13.

(IV) The fields in $\mathcal{H}_3$, $\mathcal{H}_4$, $\mathcal{H}_5$ are precisely the totally real fields with discriminant $\leq 10^6$ that satisfy conditions (a), (b), (c) of Theorem 3. For such $K \in \mathcal{H}_3 \cup \mathcal{H}_4 \cup \mathcal{H}_5$ we know that asymptotic FLT holds over any K' that is a 2-extension of K unramified away from the unique prime above 2; in particular, when $K' = K \cdot \mathbb{Q}(\zeta_{2^r})^+$.

A Variant where 2 is not totally ramified. We give an example to show how the proof of Theorem 6 can still be useful in establishing asymptotic FLT, even if 2 does not totally ramify in the field. Let K be the number field generated by a root of $x^5 + x^4 - 12x^3 - 21x^2 + x + 5$. This is totally real and has degree 5. Moreover, 2 is inert in this field, and we let $\mathfrak{P} = 2\mathcal{O}_K$. Taking $V = \mathcal{O}_K^\times$, we checked that every element of U is a square. The proof of Theorem 6 shows that if (λ, μ) is a solution to the S-unit equation, then after applying a suitable element of $\mathfrak{S}_3$, $0 \leq \mathrm{ord}_{\mathfrak{P}}(\lambda) \leq 4$ and $\mathrm{ord}_{\mathfrak{P}}(\mu) = 0$. Thus we may write $\lambda = 2^r\lambda'$ where $0 \leq r \leq 4$, and λ', μ are both units. Instead of solving the S-unit equation (5) to apply Theorem 10, we merely have to solve the (easier) unit equations $2^r\lambda' + \mu = 1$ for $0 \leq r \leq 4$. Using `Magma`'s inbuilt unit equation solver we find no solutions for $r = 0, 2, 3, 4$, and precisely one solution for $r = 1$, which $\lambda' = 1$, $\mu = -1$. Hence the only solutions to the S-unit equation (5) are the irrelevant ones. Now applying part (B) of Theorem 10 allows us to deduce asymptotic FLT for K.

Another Computational Example. Let $\{f_n\}$ be the sequence of polynomials in (2). It is easy to see that f_n is monic of degree n and belongs to $\mathbb{Z}[x]$. Let α be any root of f_n and $K_n = \mathbb{Q}(\alpha)$.

Lemma 10.1. *K_n is a totally real field of degree n in which 2 totally ramifies.*

Proof. Write $K = K_n$. Let $L = K(\sqrt{-7})$. Let $\beta \in L$ be related to α by

$$\beta = \frac{\alpha + \sqrt{-7}}{\alpha - \sqrt{-7}}, \qquad \alpha = \sqrt{-7} \cdot \frac{(\beta + 1)}{(\beta - 1)}.$$

Let $\pi_1 = (1 + \sqrt{-7})/2$ and $\pi_2 = (1 - \sqrt{-7})/2$. These are the primes above 2 in $\mathbb{Q}(\sqrt{-7})$.

From $f_n(\alpha) = 0$ it follows that $\beta^n = \pi_2/\pi_1$, so that $x^n - \pi_2/\pi_1$ is π_2-Eisenstein polynomial. We conclude π_1, π_2 are totally ramified in the degree n extension $L/\mathbb{Q}(\sqrt{-7})$, and $[L : \mathbb{Q}] = 2n$. Moreover, π_2/π_1 has complex absolute value 1 so $\sigma(\beta)$ lies on the unit circle for all embeddings $\sigma : L \hookrightarrow \mathbb{C}$. Note that the Möbius transformation $z \mapsto \sqrt{-7}\cdot(z+1)/(z-1)$ maps β to α and transforms the unit circle into the real line. Thus $\sigma(\alpha) \in \mathbb{R}$ for all the embeddings of L, so K is totally real. Moreover $L = K(\sqrt{-7})$ and so K has degree n. Finally 2 is not ramified in $\mathbb{Q}(\sqrt{-7})$, and thus the primes of K above 2 are not ramified in L/K. This allows us to deduce that 2 is totally ramified in K. □

We ran our `Magma` implementation of the criterion of Theorem 6 for these fields with $2 \le n \le 32$. Here we took V to be a subgroup of odd index in $\mathcal{O}_K^\times$. We found that every element of U is a square for precisely the following values of n: $1 \le n \le 6$, $8 \le n \le 14$, $15 \le n \le 20$, $23 \le n \le 27$, $n = 29$, 31, 32. By Theorem 6 asymptotic FLT holds over K_n for these values. We note in passing that `Magma` can compute the full unit group of K_n for $n \le 18$, but appears not to be able to do this (unconditionally) for larger values of n.

A comparison of theorems. The following lemma explains observation (II) above. Moreover, it does show that the assumptions of Theorem 6 are weaker than those of Theorem 2. Indeed, Theorem 2 is theoretically useful, but Theorem 6 is more powerful in practice.

Lemma 10.2. *Let K be a number field with exactly one prime $\mathfrak{P}$ above 2. Suppose the order of $[\mathfrak{P}] \in \mathrm{Cl}_K^+$ is divisible by $h_{K,2}^+$. Let V, U be as in Theorem 6. Then every element of U is a square.*

Proof. Let L be the narrow Hilbert 2-class field of K. By Proposition 5.2, L has exactly one prime above $\mathfrak{P}$. Let $u \in U$. We want to prove that u is a square in K. We will in fact first show that it is a square in L and then deduce that it is a square in K.

Note that $(1+\sqrt{u})/2$ satisfies the polynomial $f = X^2 - X + (1-u)/4 \in \mathcal{O}_K[x]$. Moreover, the discriminant of f is $u \in \mathcal{O}_K^\times$. It follows in particular that $K(\sqrt{u})/K$ is an extension that is unramified at the finite places, and so $K(\sqrt{u}) \subseteq L$ by definition of L. Suppose $K(\sqrt{u}) \ne K$, and write $M = K(\sqrt{u})$. Then f is the minimal polynomial of $\alpha := (1+\sqrt{u})/2 \in \mathcal{O}_M$. We will apply the Dedekind–Kummer theorem to show that $\mathfrak{P}$ splits in M. To do this, we first show that $\mathcal{O}_M = \mathcal{O}_K[\alpha]$. Indeed, by [6, Theorem 1.2.30]

$$\frac{\mathcal{O}_M}{\mathcal{O}_K[\alpha]} \cong \frac{\mathcal{O}_K}{\mathfrak{a}_1} \oplus \cdots \oplus \frac{\mathcal{O}_K}{\mathfrak{a}_r}$$

where $\mathfrak{a}_i$ are ideals of $\mathcal{O}_K$ satisfying $\mathfrak{a}_1 \mid \mathfrak{a}_2 \mid \cdots \mid \mathfrak{a}_r$. Moreover, by [6, page 79],

$$\mathrm{Disc}(f)\cdot\mathcal{O}_K = \Delta_{M/K}\cdot\mathfrak{a}_1^2\cdots\mathfrak{a}_r^2,$$

where $\Delta_{M/K} \subseteq \mathcal{O}_K$ is the relative discriminant ideal for M/K. But $\mathrm{Disc}(f) = u \in \mathcal{O}_K^\times$. It follows that the $\mathfrak{a}_i = \mathcal{O}_K$ and so $\mathcal{O}_M = \mathcal{O}_K[\alpha]$ as desired. Now $f \equiv X(X-1) \pmod{\mathfrak{P}}$. It follows from the Dedekind–Kummer theorem [6, Proposition 2.3.9] that $\mathfrak{P}$ splits in $K(\sqrt{u})$. Thus there cannot be exactly one prime above $\mathfrak{P}$ in $L \supseteq M$. This contradiction shows that $K(\sqrt{u}) = K$. □

An Explanation for (III). The following is a mild generalization of [15, Théorème 5]. It provides an explanation for observation (III) above.

Theorem 13. *Let K be a totally real field of degree 2^n for $n \geq 1$. Suppose 2 totally ramifies in K, and h_K^+ is odd. Then $K = \mathbb{Q}(\zeta_{2^{n+2}})^+$.*

Proof. We first show that every totally positive unit in K is a square. Let $d = 2^n$ for the degree of K. Write $V = \mathcal{O}_K^\times$, V^2 for the subgroup of squares in V, and V^+ for the subgroup of totally positive units. By [6, Corollary 3.2.4],

$$\frac{h_K^+}{h_K} = \frac{2^d}{[V : V^+]}.$$

As h_K^+ is odd, we have $h_K^+ = h_K$ and so $[V : V^+] = 2^d$. However, $V^2 \subseteq V^+$ and by Dirichlet's unit theorem $[V : V^2] = 2^d$. We conclude that $V^+ = V^2$. In other words, every totally positive unit of K is a square.

We now need some notation. For $r \geq 3$, write

$$\beta_r = \zeta_{2^r} + \zeta_{2^r}^{-1}, \qquad \gamma_r = \beta_r + 2, \qquad L_r = \mathbb{Q}(\beta_r) = \mathbb{Q}(\zeta_{2^r})^+.$$

Recall that the unique prime above 2 in $\mathbb{Q}(\zeta_{2^r})$ is generated by $(1 - \zeta_{2^r})$ and therefore also by its Galois conjugate $(1 + \zeta_{2^r})$. Thus the unique prime above 2 in L_r is generated by $\gamma_r = (1 + \zeta_{2^r})(1 + \zeta_{2^r}^{-1})$. We note that

$$\beta_{r+1}^2 = \gamma_r, \qquad (\gamma_r \mathcal{O}_{L_r})^{2^{r-2}} = 2\mathcal{O}_{L_r}. \tag{14}$$

It follows from these that $\gamma_r := \beta_r + 2$ is totally positive and $\gamma_r^{2^{r-2}}/2$ is a unit.

Claim: $\beta_r \in K$ for $3 \leq r \leq n + 2$.

Note that our claim implies the theorem, for applying the claim with $r = n + 2$ yields $\mathbb{Q}(\zeta_{2^{n+2}})^+ \subseteq K$, and as both fields have degree 2^n, so they must be equal.

Let $\mathfrak{P}$ be the unique prime of K above 2. Then $\mathfrak{P}^{2^n} = 2\mathcal{O}_K$. As h_K^+ is odd, we see that $\mathfrak{P} = \alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ is totally positive. Then $2/\alpha^{2^n}$ is a totally positive unit. In follows that $2/\alpha^{2^n} = s^2$ where s is a unit of K. We prove the claim by induction. Suppose $n \geq 1$ (if $n = 0$ then there is nothing to prove). Thus $\sqrt{2} = s \cdot \alpha^{2^{n-1}} \in K$. But $\beta_3 = \zeta_8 + \zeta_8^{-1} = \sqrt{2}$. This establishes our claim for $r = 3$. For the inductive step, suppose $3 \leq r \leq n + 1$ and $\beta_r \in K$. Therefore $L_r \subseteq K$ and $\gamma_r \in K$. From (14)

$$(\gamma_r \mathcal{O}_K)^{2^{r-2}} = 2\mathcal{O}_K = \mathfrak{P}^{2^n} = \left(\mathfrak{P}^{2^{n+2-r}}\right)^{2^{r-2}}.$$

Therefore

$$\gamma_r \mathcal{O}_K = \mathfrak{P}^{2^{n+2-r}} = \alpha^{2^{n+2-r}} \mathcal{O}_K.$$

Thus $\gamma_r/\alpha^{2^{n+2-r}}$ is a unit. It is totally positive, as α and γ_r are totally positive, and so must be the square of a unit, s_r^2. Hence $\beta_{r+1} = \sqrt{\gamma_r} = s_r \cdot \alpha^{2^{n+1-r}} \in K$, establishing the claim and completing the proof. □

11. Proof of Theorem 7

All the work done in this paper so far was under the assumption that the fields K considered have a unique prime above 2. In this setting our results were obtained by a careful study of the solutions to S-unit equation with the help of class field theory.

Theorem 7 concerns a family of quadratic fields having two primes above 2. We still study S-unit equation using class field theory, but that alone appears

insufficient to yield a complete proof. In particular, we will need the following proposition, whose proof makes use of the theory of linear forms in logarithms and Diophantine approximation. We postpone its proof to Section 12 so as not to disrupt the flow of the argument.

Proposition 11.1. *Let $\tau = 3 + 2\sqrt{2}$. The only solutions to the equation*

$$2^{s_1} + \eta \cdot 2^{s_2} = \frac{\tau^k - \tau^{-k}}{2\sqrt{2}}, \qquad s_1,\, s_2,\, k \geq 0, \quad s_1 \geq s_2, \quad \eta = \pm 1, \tag{15}$$

are $k = 0$, $\eta = -1$, and $s_1 = s_2$, or $(k, \eta, s_1, s_2) = (1,1,0,0)$, $(1,-1,2,1)$, $(2,1,3,2)$, $(2,-1,4,2)$.

We note that Theorem 7 follows immediately from Theorem 10 and the following lemma, so the rest of this section is devoted to its proof.

Lemma 11.2. *Let $\ell \equiv 1 \pmod{24}$ be prime, and $K = \mathbb{Q}(\sqrt{\ell})$. Write $\mathfrak{P}_1$, $\mathfrak{P}_2$ for the two primes of K above 2 and let $S = \{\mathfrak{P}_1, \mathfrak{P}_2\}$. If $\ell > 73$ then the solutions to the S-unit equation*

$$\lambda + \mu = 1, \qquad \lambda,\, \mu \in \mathcal{O}_S^\times \tag{16}$$

satisfy $\max\{|\mathrm{ord}_{\mathfrak{P}_1}(\lambda)|, |\mathrm{ord}_{\mathfrak{P}_1}(\mu)|\} = 1$ or $\max\{|\mathrm{ord}_{\mathfrak{P}_2}(\lambda)|, |\mathrm{ord}_{\mathfrak{P}_2}(\mu)|\} = 1$. If $\ell = 73$, the same conclusion holds with the exception of the $\mathfrak{S}_3$-orbit of

$$\lambda = \frac{-23 + 3\sqrt{73}}{2}, \qquad \mu = \frac{25 + 3\sqrt{73}}{2} \tag{17}$$

From now on, the notation in this section will be that of Lemma 11.2.

Lemma 11.3. *The ray class numbers $h_{\mathfrak{P}_1^2}$, $h_{\mathfrak{P}_2^2}$ are odd.*

Proof. Let $\mathfrak{P}$ be either $\mathfrak{P}_1$ or $\mathfrak{P}_2$. By (9), the class number h_K of K is odd. Note that $(\mathcal{O}_K/\mathfrak{P}^2)^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times$ is generated by the image of $-1 \in \mathcal{O}_K^\times$. Thus the natural map

$$\rho : \mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{P}^2)^\times$$

is surjective. The exact sequence in [6, Proposition 3.2.3] tells us that $h_{\mathfrak{P}^2} = h_K$. □

Recall that the solutions $(1/2, 1/2)$, $(-1, 2)$ and $(2, -1)$ to (16) are called irrelevant, and the other solutions are called relevant. We would like to understand the relevant solutions. For the following, see [9, Lemma 6.4] and its proof.

Lemma 11.4. *Up to the action of $\mathfrak{S}_3$, every relevant solution (λ, μ) of (16) has the form*

$$\lambda = \frac{\eta_1 \cdot 2^{r_1} - \eta_2 \cdot 2^{r_2} + 1 + v\sqrt{\ell}}{2}, \qquad \mu = \frac{\eta_2 \cdot 2^{r_2} - \eta_1 \cdot 2^{r_1} + 1 - v\sqrt{\ell}}{2} \tag{18}$$

where

$$\eta_1 = \pm 1, \qquad \eta_2 = \pm 1, \qquad r_1 \geq r_2 \geq 0, \qquad v \in \mathbb{Z}, \qquad v \neq 0 \tag{19}$$

are related by

$$(\eta_1 \cdot 2^{r_1} - \eta_2 \cdot 2^{r_2} + 1)^2 - \eta_1 \cdot 2^{r_1+2} = \ell v^2, \tag{20}$$

$$(\eta_2 \cdot 2^{r_2} - \eta_1 \cdot 2^{r_1} + 1)^2 - \eta_2 \cdot 2^{r_2+2} = \ell v^2. \tag{21}$$

Moreover,

$$\mathrm{Norm}_{K/\mathbb{Q}}(\lambda) = \eta_1 \cdot 2^{r_1}, \qquad \mathrm{Norm}_{K/\mathbb{Q}}(\mu) = \eta_2 \cdot 2^{r_2}. \tag{22}$$

Lemma 11.5. *Let (λ,μ), η_i, r_i be as in Lemma 11.4 with $r_1 \le 5$. Then $\ell = 73$ and (λ,μ) is given by* (17).

Proof. This is a straightforward computation as $r_2 \le r_1$. □

We shall henceforth suppose that $r_1 \ge 6$.

Lemma 11.6. *Let (λ,μ), η_i, r_i be as in Lemma 11.4. Then, for $i = 1, 2$, we have*

$$\eta_i = -1 \iff r_i \equiv 1 \pmod 2.$$

Proof. Let $a = \eta_1 \cdot 2^{r_1}$ and $b = \eta_2 \cdot 2^{r_2}$. Equation (20) becomes

$$(a-b+1)^2 - 4a = \ell v^2.$$

We consider this modulo 3. Since $\ell \equiv 1 \pmod 3$ we infer

$$(a-b+1)^2 - a \equiv 0 \text{ or } 1 \pmod 3. \tag{23}$$

However $(a,b) \equiv (\pm 1, \pm 1) \pmod 3$. Of these four possibilities for (a,b) modulo 3, the only one that satisfies (23) is $(a,b) \equiv (1,1) \mod 3$. Thus $2^{r_i} \equiv \eta_i \pmod 3$ for $i = 1, 2$. This gives the lemma. □

Lemma 11.7. *Let (λ,μ), η_i, r_i be as in Lemma 11.4. Then $r_2 > 0$.*

Proof. Suppose $r_2 = 0$. By Lemma 11.6 we have $\eta_2 = 1$. Now (20) becomes

$$2^{2r_1} - \eta_1 \cdot 2^{r_1+2} = \ell v^2.$$

The 2-adic valuation of the left-hand side is $r_1 + 2$, and this must be even in view of the right-hand side. Moreover, by Lemma 11.6 we have $\eta_1 = 1$. Removing a factor of 2^{r_1+2} from both sides gives

$$2^{r_1-2} - 1 = \ell w^2, \qquad w \in \mathbb{Z}.$$

This is impossible modulo 4. □

Since the residue field of $\mathfrak{P}_i$ is $\mathbb{F}_2$ and $\lambda + \mu = 1$ we have $\mathfrak{P}_i$ divides λ or μ but not both. In particular $\max\{\mathrm{ord}_{\mathfrak{P}_i}(\lambda), \mathrm{ord}_{\mathfrak{P}_i}(\mu)\} \ge 1$ for $i = 1, 2$. As we would like to prove Lemma 11.2 we shall suppose that $\max\{\mathrm{ord}_{\mathfrak{P}_i}(\lambda), \mathrm{ord}_{\mathfrak{P}_i}(\mu)\} \ge 2$ for $i = 1, 2$. From (22), if $\mathfrak{P}_1$, $\mathfrak{P}_2$ both divide λ then $r_2 = 0$, and if both divide μ then $r_1 = 0$, which contradict Lemma 11.7. Hence, after possibly swapping $\mathfrak{P}_1$, $\mathfrak{P}_2$ we have,

$$\begin{cases} \mathrm{ord}_{\mathfrak{P}_2}(\lambda) = \mathrm{ord}_{\mathfrak{P}_1}(\mu) = 0, \quad \mathrm{ord}_{\mathfrak{P}_1}(\lambda) = r_1, \quad \mathrm{ord}_{\mathfrak{P}_2}(\mu) = r_2, \\ r_1 \ge r_2, \quad r_1 \ge 6, \quad r_2 \ge 2. \end{cases} \tag{24}$$

Lemma 11.8. *Let $\eta = \pm 1$. The only solutions to the equation $a^2 - b^2 = \eta \cdot 2^k$ in positive odd integers a, b are*

$$a = 2^{k-2} + \eta, \qquad b = 2^{k-2} - \eta$$

with $k \ge 3$.

Proof. Observe that $a^2 - b^2 \equiv 0 \pmod 8$ and so $k \ge 3$. It is sufficient to prove the lemma for $\eta = 1$. Then $(a+b)(a-b) = 2^k$, and so

$$a + b = 2^s, \qquad a - b = 2^t, \qquad 1 \le t < s, \qquad s + t = k.$$

Then $b = 2^{s-1} - 2^{t-1}$ and as b is odd we have $t = 1$, and so $s = k - 1$. □

Lemma 11.9. $\eta_1 = \eta_2 = -1$.

Proof. Suppose $\eta_1 = 1$. Thus $r_1 = 2s$ by Lemma 11.6. From (20) we have

$$(2^{2s} + 2^{s+1} + 1 - \eta_2 2^{r_2})(2^{2s} - 2^{s+1} + 1 - \eta_2 2^{r_2}) = \ell v^2.$$

The two factors are coprime. Moreover, as $2s = r_1 \geq r_2$ we see that the first factor is positive, and so the second must be positive. Hence

$$\text{Case I:} \quad 2^{2s} + 2^{s+1} + 1 - \eta_2 2^{r_2} = x^2, \qquad 2^{2s} - 2^{s+1} + 1 - \eta_2 2^{r_2} = \ell y^2$$

or

$$\text{Case II:} \quad 2^{2s} + 2^{s+1} + 1 - \eta_2 2^{r_2} = \ell y^2, \qquad 2^{2s} - 2^{s+1} + 1 - \eta_2 2^{r_2} = x^2$$

for some positive integers x, y.

Let

$$\eta_3 = \begin{cases} 1 & \text{Case I} \\ -1 & \text{Case II.} \end{cases}$$

Then we may rewrite our equations as

$$(2^s + \eta_3)^2 - x^2 = \eta_2 2^{r_2}, \qquad 2^{2s} - \eta_3 2^{s+1} + 1 - \eta_2 2^{r_2} = \ell y^2. \tag{25}$$

We apply Lemma 11.8 to the first equation in (25). This gives us

$$2^s + \eta_3 = 2^{r_2 - 2} + \eta_2,$$

and $r_2 \geq 3$. Recall that $r_1 \geq 6$. Thus $s \geq 3$. Hence $\eta_3 = \eta_2$ and $s = r_2 - 2$. Substituting into the second equation in (25) we obtain

$$2^{2r_2 - 4} - 3\eta_2 \cdot 2^{r_2 - 1} + 1 = \ell y^2.$$

Thus $\ell y^2 \equiv 2 \pmod 3$, which is impossible. This completes the proof that $\eta_1 = -1$.

It remains to show that $\eta_2 = -1$. Thus suppose $\eta_2 = 1$, hence r_2 is even and we write $r_2 = 2s$. Now we use (21), which we can rewrite as

$$(2^{2s} + 2^{s+1} + 1 + 2^{r_1})(2^{2s} - 2^{s+1} + 1 + 2^{r_1}) = \ell v^2.$$

the factors are positive and coprime. Now the proof is exactly as before. □

From Lemma 11.9 and Lemma 11.6 we know now that r_1, r_2 are odd. We shall write $r_i = 2s_i + 1$. We can now make (22) more precise:

$$\text{Norm}(\lambda) = -2^{2s_1 + 1}, \qquad \text{Norm}(\mu) = -2^{2s_2 + 1}. \tag{26}$$

We shall denote Galois conjugation in K by $x \mapsto \overline{x}$.

Lemma 11.10. *$\lambda\overline{\mu}$ is totally positive (i.e. positive in both embeddings).*

Proof. Let σ_1, $\sigma_2 : K \hookrightarrow \mathbb{R}$ be the two embeddings. Let $\lambda_i = \sigma_i(\lambda)$ and $\mu_i = \sigma_i(\mu)$. We are required to show that $\lambda_1\mu_2 > 0$ and $\lambda_2\mu_1 > 0$. From (26)

$$\lambda_1\lambda_2 < 0, \qquad \mu_1\mu_2 < 0.$$

Moreover as $\lambda + \mu = 1$ we have $\lambda_1 + \mu_1 = 1$ and $\lambda_2 + \mu_2 = 1$. Thus λ_1, μ_1 cannot both be negative, and λ_2, μ_2 cannot both be negative. Examining all the possible signs we find that $\lambda_1\mu_2$ and $\lambda_2\mu_1$ are both positive. □

Lemma 11.11. *$\lambda\overline{\mu} = \varepsilon^2$ for some $\varepsilon \in \mathcal{O}_K$.*

Proof. We shall study the ramification for $K(\sqrt{\lambda\overline{\mu}})/K$. Note that $\lambda\overline{\mu}$ is totally positive by Lemma 11.10, thus $K(\sqrt{\lambda\overline{\mu}})/K$ is unramified at the infinite places. Moreover, it is unramified at all finite $\mathfrak{q} \nmid 2$ as $\lambda\overline{\mu} \in \mathcal{O}_S^\times$. To study ramification at $\mathfrak{P}_1$, $\mathfrak{P}_2$. Note that $K_{\mathfrak{P}_1} = K_{\mathfrak{P}_2} = \mathbb{Q}_2$. There are seven quadratic extensions of $\mathbb{Q}_2$ obtained by adjoining the square-root of one of 5, 3, 7, 2, 6, 10, 14, and these have discriminants 1, 2^2, 2^2, 2^3, 2^3, 2^3, 2^3 respectively. As $\mathfrak{P}_2 = \overline{\mathfrak{P}_1}$, we see from the valuations in (24) that

$$\lambda\overline{\mu} = (1-\mu)\cdot(1-\overline{\lambda}) \equiv 1 \pmod{\mathfrak{P}_2^{r_2}}.$$

Thus $\mathfrak{P}_2$ does not ramify in $K(\sqrt{\lambda\overline{\mu}})$. It remains to measure the ramification at $\mathfrak{P}_1$. However, $\mathrm{ord}_{\mathfrak{P}_1}(\lambda\overline{\mu}) = r_1 + r_2$. From Lemma 11.9, and Lemma 11.6, we have $r_1 \equiv r_2 \equiv 1 \pmod 2$, and so $2 \mid (r_1 + r_2)$. We deduce that the discriminant of $K(\sqrt{\lambda\overline{\mu}})/K$ divides $\mathfrak{P}_1^2$. As the ray class number for the modulus $\mathfrak{P}_1^2$ is odd (Lemma 11.3), we deduce that $K(\sqrt{\lambda\overline{\mu}}) = K$. □

We now complete the proof of Lemma 11.2. From (26)

$$1 = (\lambda+\mu)(\overline{\lambda}+\overline{\mu}) = -2^{2s_1+1} - 2^{2s_2+1} + \lambda\overline{\mu} + \overline{\lambda}\mu.$$

Thus

$$\varepsilon^2 + \overline{\varepsilon}^2 = 2^{2s_1+1} + 2^{2s_2+1} + 1. \tag{27}$$

However,

$$(\varepsilon\overline{\varepsilon})^2 = \mathrm{Norm}(\varepsilon^2) = \mathrm{Norm}(\lambda\mu) = 2^{2s_1+2s_2+2}.$$

Thus

$$\varepsilon\overline{\varepsilon} = \eta\cdot 2^{s_1+s_2+1}, \qquad \eta = \pm 1. \tag{28}$$

Recall $K = \mathbb{Q}(\sqrt{\ell})$ with $\ell \equiv 1 \pmod{24}$. As $\varepsilon \in \mathcal{O}_K$ we may write

$$\varepsilon = \frac{w_1 + w_2\sqrt{\ell}}{2}$$

where $w_1, w_2 \in \mathbb{Z}$, and $w_1 \equiv w_2 \pmod 2$. Now (27) and (28) can be rewritten as

$$\frac{w_1^2 + \ell w_2^2}{2} = 2^{2s_1+1} + 2^{2s_2+1} + 1, \qquad \frac{w_1^2 - \ell w_2^2}{2} = \eta\cdot 2^{s_1+s_2+2}. \tag{29}$$

Hence

$$w_1^2 = 2^{2s_1+1} + \eta\cdot 2^{s_1+s_2+2} + 2^{2s_2+1} + 1 = 2\cdot(2^{s_1} + \eta\cdot 2^{s_2})^2 + 1, \tag{30}$$

and

$$\ell w_2^2 = 2^{2s_1+1} + 2^{2s_2+1} + 1 - \eta\cdot 2^{s_1+s_2+2}. \tag{31}$$

We rewrite (30) as

$$w_1^2 - 2\cdot(2^{s_1} + \eta\cdot 2^{s_2})^2 = 1.$$

It follows that $|w_1| + (2^{s_1} + \eta\cdot 2^{s_2})\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$. The units of this ring have the form $\pm(1+\sqrt{2})^u$. However, as $1+\sqrt{2}$ has norm -1, we deduce that

$$|w_1| + (2^{s_1} + \eta\cdot 2^{s_2})\sqrt{2} = \tau^k, \tag{32}$$

where $\tau = (1+\sqrt{2})^2 = 3 + 2\sqrt{2}$ and k is a non-negative integer. Hence

$$2^{s_1} + \eta\cdot 2^{s_2} = \frac{\tau^k - \tau^{-k}}{2\sqrt{2}}.$$

We now apply Proposition 11.1 to deduce that $k = 0$, $\eta = -1$ and $s_1 = s_2$ (the other solutions in the proposition lead either to the solution (17) or to contradictions with (31) using $\ell \equiv 1 \pmod{24}$). From (31) we obtain

$$\ell w_2^2 = 2^{2s_1+3} + 1 = 8 \times 4^{s_1} + 1.$$

The right-hand side is divisible by 3, and so $3 \mid w_2$. Thus the right-hand side must be divisible by 9. But the right-hand is 0, 6 or 3 modulo 9 according to whether $s_1 \equiv 0$, 1 or 2 $\pmod 3$. Hence $3 \mid s_1$. Write $s_1 = 3t$. Then

$$\ell w_2^2 = (2^{2t+1})^3 + 1 = (2^{2t+1} + 1)(2^{4t+2} - 2^{2t+1} + 1).$$

The greatest common divisor of the two factors on the right-hand side is 3. Hence either $2^{2t+1} + 1 = 3x^2$, or $2^{4t+2} - 2^{2t+1} + 1 = 3x^2$, for some integer x. However, both equations are impossible modulo 4, as long as $t \geq 1$. If $t = 0$ then $\ell w_2^2 = 9$ which is also impossible. This completes the proof of Lemma 11.2 and therefore of Theorem 7.

12. A Diophantine Problem: Proof of Proposition 11.1

In Section 11 we used class field theory to reduce the proof of Theorem 7 to the Diophantine problem in Proposition 11.1. We will now give a proof of that proposition. Throughout this section (k, η, s_1, s_2) will be a solution to (15). The conclusion of Proposition 11.1 is clear when $k = 0$. Therefore assume that $k \geq 1$.

Lemma 12.1. $s_2 \leq \mathrm{ord}_2(k) + 1$.

Proof. We work in $\mathbb{Z}[\sqrt{2}]$. We claim that

$$\mathrm{ord}_{\sqrt{2}}(\tau^{2^a} - 1) = 2a + 3, \qquad \text{for all } a \geq 1.$$

This is true for $a = 1$, and claim is easily established by induction using the identity

$$\tau^{2^{a+1}} - 1 = 2 \cdot \left(\tau^{2^a} - 1\right) + \left(\tau^{2^a} - 1\right)^2.$$

Write $k = 2^b \cdot k_0$ where k_0 is odd. From (15) we deduce that

$$(\tau^{2^{b+1}})^{k_0} = \tau^{2k} \equiv 1 \pmod{\sqrt{2}^{2s_2+3}}.$$

But, using the standard number field generalization of the Euler totient function,

$$\#\left(\mathbb{Z}[\sqrt{2}]/\sqrt{2}^{2s_2+3}\right)^\times = \mathrm{Norm}\left(\sqrt{2}^{2s_2+3}\right) - \mathrm{Norm}\left(\sqrt{2}^{2s_2+2}\right) = 2^{2s_2+2},$$

and in particular is coprime to k_0. Thus

$$\tau^{2^{b+1}} \equiv 1 \pmod{\sqrt{2}^{2s_2+3}}.$$

We deduce that

$$2s_2 + 3 \leq \mathrm{ord}_{\sqrt{2}}\left(\tau^{2^{b+1}} - 1\right) = 2(b+1) + 3,$$

so $\mathrm{ord}_2(k) = b \geq s_2 - 1$ completing the proof. □

Lemma 12.2. *The only solutions to* (15) *with* $k \leq 10^3$ *are as given in Proposition 11.1.*

Proof. Let $P_k = (\tau^k - \tau^{-k})/2\sqrt{2} \in \mathbb{Z}$. For each value $1 \le k \le 10^3$, Lemma 12.1 gives us $s_2 \le \mathrm{ord}_2(k) + 1$. In view of (15), we need only check for the possible values of k, s_2, and $\eta = \pm 1$, if $P_k - \eta \cdot 2^{s_2}$ is a power of 2. We wrote a `Magma` script which did this and the only solutions we found are $(k, \eta, s_1, s_2) = (1, 1, 0, 0)$, $(1, -1, 2, 1)$, $(2, 1, 3, 2)$, $(2, -1, 4, 2)$. □

We will therefore henceforth assume that $k > 1000$. This makes the forthcoming inequalities easier to deal with. Next we apply the theory of linear forms in logarithms to obtain a bound on k. We know that $2^{s_2} \le 2k$ by Lemma 12.1. From (15) we obtain

$$\left|\sqrt{2}^{2s_1+3} - \tau^k\right| \le 2^{s_2+1} \cdot \sqrt{2} + \tau^{-k} \le 4\sqrt{2} \cdot k + \tau^{-k} < 6k.$$

Hence

$$\left|\frac{\sqrt{2}^{2s_1+3}}{\tau^k} - 1\right| < \frac{6k}{\tau^k}. \tag{33}$$

Let

$$\Lambda = (2s_1 + 3) \cdot \log(\sqrt{2}) - k \cdot \log(\tau). \tag{34}$$

Using the elementary inequality $|\log(1 + x)| \le 2x$ for $|x| \le 1/2$, where we take $x = \exp(\Lambda) - 1$, we obtain

$$|\Lambda| < \frac{12k}{\tau^k}. \tag{35}$$

Hence

$$2s_1 + 3 < \left(\frac{\log(\tau)}{\log(\sqrt{2})} + \frac{12}{\log(\sqrt{2}) \cdot \tau^{1000}}\right) \cdot k < 6k. \tag{36}$$

We now apply the theorem of Baker and Wüstholz for linear forms in logarithms [25, page 225], where in the notation of that theorem we take:

$$\alpha_1 = \sqrt{2}, \quad \alpha_2 = \tau, \quad n = d = 2, \quad b_1 = 2s_1 + 3, \quad b_2 = -k, \quad B = \max\{2s_1 + 3, k\}.$$

We find in the notation of that theorem (see also [25, page 22]) that

$$h_m(\alpha_1) = \frac{1}{2}, \quad h_m(\alpha_2) = \frac{\log(3 + 2\sqrt{2})}{2}.$$

The theorem gives

$$\log|\Lambda| > -C \cdot \log B, \tag{37}$$

where

$$C = 18(n+1)! \cdot n^{n+1} \cdot (32d)^{n+2} \cdot \log(2nd) \cdot h_m(\alpha_1) \cdot h_m(\alpha_2) < 1.33 \cdot 10^{10}.$$

From (36) we have

$$B < 6k.$$

Thus from (35) and (37) we obtain

$$\log k + \log 12 - k \cdot \log \tau > -C \cdot \log k - C \cdot \log 6.$$

Thus

$$k < \frac{C+1}{\log \tau} \cdot \log k + \frac{C \cdot \log 6 + \log 12}{\log \tau} < a + b \log k$$

where $a = 1.36 \times 10^{10}$ and $b = 7.55 \times 10^9$. Now Lemma B.1 of [25, Appendix B] gives

$$k < 2(a + b \log b) < 3.8 \times 10^{11}. \tag{38}$$

From (34) and (35) we find

$$\left|\frac{2s_1+3}{k} - \frac{\log\tau}{\log\sqrt{2}}\right| < \frac{12}{\log\sqrt{2}}\cdot\frac{1}{\tau^k}. \tag{39}$$

We computed using `PARI/GP` the first 30 terms of the continued fraction expansion of $\log\tau/\log\sqrt{2}$, and found that the 30-th convergent is p/q where

$$p = 1815871259660093, \qquad q = 357018312787640 \approx 3.57\times 10^{14}.$$

Then

$$\left|\frac{p}{q} - \frac{\log\tau}{\log\sqrt{2}}\right| < \frac{1}{q^2}. \tag{40}$$

Therefore

$$\left|\frac{p}{q} - \frac{2s_1+3}{k}\right| < \frac{1}{q^2} + \frac{12}{\log\sqrt{2}}\cdot\frac{1}{\tau^k}.$$

If $p/q = (2s_1+3)/k$ then $q \mid k$ contradicting (38). Thus $p/q \neq (2s_1+3)/k$ and so $|p/q - (2s_1+3)/k| \geq 1/qk$. Thus

$$\frac{1}{qk} < \frac{1}{q^2} + \frac{12}{\log\sqrt{2}}\cdot\frac{1}{\tau^k}.$$

From (38), $1/(2k) > 1/q$ and so,

$$\frac{1}{2qk} < \frac{12}{\log\sqrt{2}}\cdot\frac{1}{\tau^k}$$

and thus

$$k < \frac{1}{\log\tau}\cdot\log k + \frac{1}{\log\tau}\cdot\log\left(\frac{24q}{\log\sqrt{2}}\right).$$

Applying Lemma B.1 of [25, Appendix B] now gives $k < 73$. In view of Lemma 12.2, this completes the proof of Proposition 11.1.

References

[1] J.-F. Biasse and C. Fieker, *Improved techniques for computing the ideal class group and a system of fundamental units in number fields*, ANTS XProceedings of the Tenth Algorithmic Number Theory Symposium, 113–133, Open Book Ser., **1**, Math. Sci. Publ., Berkeley, CA, 2013.

[2] M. Bhargava, A. Shankar, J. Tsimerman, *On the Davenport-Heilbronn theorems and second order terms*, Invent. Math. **193** (2013), no. 2, 439–499.

[3] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: the user language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://magma.maths.usyd.edu.au/magma/`)

[4] J. Browkin, *The abc-conjecture for Algebraic Numbers*, Acta Math. Sinica, English series **22** (2006), 211–222.

[5] J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres, Paris 1988–1989, 27–41, Progr. Math. **91**, Birkhäuser Boston, Boston, MA, 1990.

[6] H. Cohen, *Advanced topics in computational number theory*, GTM **138**, Springer Verlag, 2000.

[7] H. Cohen, F. Diaz y Diaz and M. Olivier, *Subexponential algorithms for class group and unit computations*, J. Symb. Comp. **24** (1997), 433–441.

[8] H. Cohn, *The density of abelian cubic fields*, Proc. Amer. Math. Soc. **5**, (1954) 476–477.

[9] N. Freitas and S. Siksek, *The asymptotic Fermat's last theorem for five-sixths of real quadratic fields*, Compos. Math. **151** (2015), no. 8, 1395–1415.

[10] N. Freitas and S. Siksek, *Fermat's Last Theorem over some small real quadratic fields*, Algebra & Number Theory **9** (2015), no. 4, 875–895.

[11] G. Hanrot, *Solving Thue equations without the full unit group*, Math. Comp. **69** (2000), no. 229, 395–405.
[12] W. Ho, A. Shankar and I. Varma, *Odd degree number fields with odd class number*, Duke Math. J. **167** (2018), 995–1047.
[13] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.
[14] F. Jarvis and P. Meekin, *The Fermat equation over* $\mathbb{Q}(\sqrt{2})$, J. Number Theory **109** (2004), no. 1, 182–196.
[15] A. Kraus, *Le théorème de Fermat sur certains corps de nombres totalement réels*, Algebra & Number Theory, to appear.
[16] H. W. Lenstra, P. Stevenhagen, *Class Field Theory and the First Case of Fermats Last Theorem*, in G. Cornell, J. H. Silverman and G. Stevens (eds) *Modular Forms and Fermats Last Theorem*, Springer, New York, 1997.
[17] F. Lemmermeyer, *Class Field Towers*, preprint, 111 pages, September 7, 2010.
[18] J. W. Jones and D. P. Roberts, *A database of number fields*, LMS J. Comput. Math. **17** (2014), no. 1, 595–618. (See also `https://hobbes.la.asu.edu/NFDB/`)
[19] G. N. Markšaĭtis, *On p-extensions with one critical number*, Izv. Akad. Nauk SSSR Ser. Mat. **27** (1963), 463–466.
[20] The PARI Group, PARI/GP version `2.11.0`, Univ. Bordeaux, 2018, `http://pari.math.u-bordeaux.fr/`.
[21] F. Pop, *Embedding problems over large fields*, Ann. of Math. (2) **144** (1996), no. 1, 1–34.
[22] M. H. Şengün and S. Siksek, *On the asymptotic Fermat's Last Theorem over numbers fields*, Commentarii Mathematici Helvetici **93** (2018), 359–375.
[23] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, Addison-Wesley Publ. Co., Reading, Mass., 1989.
[24] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM **151**, Springer, 1994.
[25] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, Cambridge University Press, 1998.
[26] M. Suzuki, *Group Theory I*, Grundlehren der mathematischen Wissenschaften **247**, Springer, Berlin, 1982.
[27] K. Takeuchi, *Arithmetic Fuchsian groups with signature* $(1; e)$, J. Math. Soc. Japan **35** (1983), no. 3, 381–407.
[28] J. Thorne, *Elliptic curves over* $\mathbb{Q}_\infty$ *are modular*, to appear in JEMS.
[29] G. Turcas, *On Fermats equation over some quadratic imaginary number fields*, Res. Number Theory **4** (2018), no. 2, Art. 24, 16 pp.
[30] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83**, Springer, 1982.
[31] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

Mathematics Institute, University of Warwick, CV4 7AL, United Kingdom
Email address: `nunobfreitas@gmail.com`

Sorbonne Université, Institut de Mathématiques de Jussieu - Paris Rive Gauche, UMR 7586 CNRS - Paris Diderot, 4 Place Jussieu, 75005 Paris, France
Email address: `alain.kraus@imj-prg.fr`

Mathematics Institute, University of Warwick, CV4 7AL, United Kingdom
Email address: `s.siksek@warwick.ac.uk`