# $S$-UNIT EQUATIONS AND THE ASYMPTOTIC FERMAT CONJECTURE OVER NUMBER FIELDS

EKIN OZMAN AND SAMIR SIKSEK

Abstract. Recent attempts at studying the Fermat equation over number fields have uncovered an unexpected and powerful connection with $S$-unit equations. In this expository paper we explain this connection and its implications for the asymptotic Fermat conjecture.

## 1. Introduction

Every mathematician is familiar with the statement of Fermat's Last Theorem, proved by Wiles and Taylor [Wil95], [TW95] in 1994.

**Theorem 1.1** (Wiles)**.** *Let $p \geq 3$ be a prime. Then the only solutions to the equation*

$$x^p + y^p + z^p = 0 \tag{1.1}$$

*with $x$, $y$, $z \in \mathbb{Q}$ satisfy $xyz = 0$.*

This survey is concerned with generalizations of Fermat's Last Theorem where $\mathbb{Q}$ is replaced by a number field $K$, and also with similar Fermat-type equations where $A, B, C$ are in the ring of integers $\mathcal{O}_K$ of $K$:

$$Ax^p + By^p + Cz^p = 0, \qquad Ax^p + By^p = Cz^2, \qquad Ax^p + By^p = Cz^3, \tag{1.2}$$

again over number fields. Interest in the Fermat equation (1.1) over number fields goes back to the 19th century and early 20th century. Dickson [Dic66, pages 758 and 768] in his monumental *History of the Theory of Numbers*, surveys the early history and mentions the efforts of Maillet (1897) and Furtwängler (1910) who extended Kummer's cyclotomic approach to the Fermat equation over $\mathbb{Q}(\zeta_p)$. Later, Hao and Parry [HP84] used the Kummer approach to prove several results concerning the exponent $p$ Fermat equation (1.1) over a quadratic field $\mathbb{Q}(\sqrt{d})$ subject to the condition that the prime $p$ does not divide the class number of $\mathbb{Q}(\sqrt{d}, \zeta_p)$. The following theorem is due to Kolyvagin [Kol01], and is a beautiful example of how far the cyclotomic approach can be pushed.

**Theorem 1.2** (Kolyvagin)**.** *Let $p \geq 5$ be a prime and write $\zeta_p$ for a primitive $p$-th root of unity. Let $x$, $y$, $z \in \mathbb{Z}[\zeta_p]$ satisfy* (1.1)*, with $(1 - \zeta_p) \nmid xyz$ (such a solution is called a 'first case solution'). Then $p^2 \mid (q^p - q)$ for all primes $q \leq 89$ with $q \neq p$.*

*Date*: October 28, 2021.

2010 *Mathematics Subject Classification.* 11D41, 11G05, 11D61.

*Key words and phrases.* S-Unit Equations, Diophantine Equations, Fermat Equation.

Ozman is partially supported by TUBITAK Research Grant 117F045 and Max Planck Institute for Mathematics (MPIM) and would like to thank MPIM for providing excellent research facilities. Siksek is supported by EPSRC grant *Moduli of Elliptic curves and Classical Diophantine Problems* (EP/S031537/1).

Another historically popular approach is to fix a prime exponent $p$ and consider points of low degree (i.e. points defined over number fields of low degree) on the Fermat curve $x^p + y^p + z^p = 0$. For example, Gross and Rohrlich [GR78] determine all points on the Fermat curve $F_p : x^p + y^p + z^p = 0$ for $p = 3, 5, 7, 11$ over all number fields $K$ of degree $\leq (p-1)/2$ through studying the Mordell–Weil group of the Jacobian of $F_p$.

After Wiles' proof of Fermat's Last Theorem using Galois representations and modularity, others tried to extend this approach to various number fields. The first result along these lines is due to Jarvis and Meekin [JM04] stating that the only solutions to (1.1) with $x, y, z \in \mathbb{Q}(\sqrt{2})$ satisfy $xyz = 0$. This was later extended to some real quadratic fields of small discriminant by Freitas and Siksek [FS15c], and to some imaginary quadratic fields of small discriminant by Turçaş [Ţur18] (the later being conditional on some standard conjectures in the Langlands programme).

Let $K$ be a number field. We say that a solution $(x, y, z) \in K^3$ to the Fermat equation (1.1) is **trivial** if $xyz = 0$ and **non-trivial** if $xyz \neq 0$. In this survey we are primarily concerned with the following conjecture, which appears to have first been formulated in [FKS20a].

**Conjecture 1.3** (The Asymptotic Fermat Conjecture)**.** *Let $K$ be a number field, and suppose the primitive third root of unity, $\zeta_3 \notin K$. There exists a constant $\mathcal{B}_K$ depending only on $K$ such that for all primes $p > \mathcal{B}_K$ the only solutions to the Fermat equation* (1.1) *with $(x, y, z) \in K^3$ are the trivial solutions.*

We remark that the asymptotic Fermat conjecture follows from a suitable version of the *ABC*-conjecture over number fields [Bro06].

**Remarks.**

- Observe that for $p \neq 3$ we have $1^p + \zeta_3^p + \zeta_3^{2p} = 0$. For this reason it is necessary to exclude number fields containing $\zeta_3$ in the statement of the conjecture.
- We cannot expect the statement of Fermat's Last Theorem to be true over every number field without modification. Indeed, fix the exponent $p$ for now. The Fermat curve $F_p : x^p + y^p + z^p = 0$ contains the rational point $(1 : -1 : 0)$. Now take a line defined over $\mathbb{Q}$ through this point. This must intersect $F_p$ in a further $p-1$ points. We see that $F_p$ has an infinite family of points defined over number fields of degree $\leq p-1$. It therefore makes sense to consider the Fermat equation over a given number field asymptotically, i.e. for large exponents $p$.
- Debarre and Klassen [DK94] suggest that the only points on the degree $p$ Fermat curve (1.1) over number fields of degree $d \leq p - 2$ lie on the line $x + y + z = 0$. Observe that the six obvious points $(1 : -1 : 0)$, $(1 : \zeta_3 : \zeta_3^2)$, and their permutations, do lie on this line.

We are grateful to the referees for many useful comments.

## 2. The Modular Approach—An Example of Serre and Mazur

As we shall see later, it is often possible to relate non-trivial solutions to Fermat-type equations to solutions to certain $S$-unit equations. In this section we sketch the earliest instance of this phenomena, which is an example due to Serre and Mazur,

given in Serre's 1987 Duke article where he formulated his famous modularity conjecture [Ser87]. The sketch will be slightly technical, and the reader unfamiliar with Galois representations and modularity should feel free to skim through it. Good introductions to the subject include [BMS16] and [Sik12].

Let $L$ be either 1 or an odd prime. Let $(x, y, z) \in \mathbb{Z}^3$ be a non-trivial solution to the equation

$$x^p + y^p + L^r z^p = 0 \tag{2.1}$$

where the exponent $p \neq L$ is a prime $\geq 5$ and $r$ is a non-negative integer. Moreover we may (after suitable scaling and possible rearrangement of the variables) suppose that $\gcd(x, y, Lz) = 1$. We suppose $r < p$ since we can absorb $p$-th powers of $L$ into $z^p$. Note that we allow $L = 1$ as we would like to include Fermat's Last Theorem in our sketch. We let $A$, $B$, $C$ be the three terms $x^p$, $y^p$, $L^r z^p$ arranged so that $A \equiv -1 \pmod 4$ and $2 \mid B$. Let $E'$ be the Frey elliptic curve

$$E' \ : \ Y^2 = X(X - A)(X + B).$$

Serre studies the mod $p$ representation $\overline{\rho}_{E',p}$ of $E'$, which is irreducible by Mazur's isogeny theorem. It follows from theorems of Ribet and Wiles that the representation $\overline{\rho}_{E',p}$ arises from a cuspidal newform $f$ with trivial character of weight 2 and level $N = 2L$. If $L = 1$ (the FLT case) then $N = 2$. However, there are no newforms of weight 2 and level 2, which gives a contradiction, and so there are no non-trivial solutions for $L = 1$. The proof of Fermat's Last Theorem is complete at this point. In fact there are no newforms of weight 2 and levels 6, 10, 22. Thus for $L = 3$, 5, 11 we can also conclude that there are no non-trivial solutions to (2.1). However, it is easy to deduce from the dimension formula for newform spaces [Coh07, Proposition 15.1.1] that there are newforms of weight 2 and level $2L$ for all other odd prime values $L = 7, 13, 17, 19, \ldots$. To progress we need to know a little about the relationship between $E'$ and the newform $f$. The newform $f$ has a $q$-expansion

$$f = q + \sum_{n=1}^{\infty} c_n q^n.$$

The coefficients $c_n$ generate a totally real field $K_f$ and in fact belong to the ring of integers $\mathcal{O}$ of $K_f$. There is some prime ideal $\varpi$ of $\mathcal{O}$ dividing $p$ so that for any prime $\ell \nmid 2Lp$ the following relations hold

$$\begin{cases} a_\ell(E') \equiv c_\ell \pmod{\varpi} & \text{if } \ell \nmid xyz \\ \pm(\ell + 1) \equiv c_\ell \pmod{\varpi} & \text{if } \ell \mid xyz. \end{cases}$$

We do not know the elliptic curve $E'$ as this depends on a hypothetical solution $(x, y, z)$ to (2.1). However, given $\ell \nmid 2L$, the trace $a_\ell(E')$ is an integer belonging to the Hasse interval $[-2\sqrt{\ell}, 2\sqrt{\ell}]$. It follows from the above congruences that $\varpi$ divides

$$\beta_\ell := \ell \cdot (\ell + 1 - c_\ell) \cdot (\ell + 1 + c_\ell) \cdot \prod_{-2\sqrt{\ell} \leq a \leq 2\sqrt{\ell}} (a - c_\ell).$$

As $\varpi$ is a prime ideal dividing $p$ it follows that $p \mid B_\ell$ where $B_\ell = \mathrm{Norm}_{K_f/\mathbb{Q}}(\beta_\ell)$. This gives a bound for the exponent $p$ provided $B_\ell \neq 0$ or equivalently $\beta_\ell \neq 0$. Note that if $c_\ell \notin \mathbb{Q}$ then $\beta_\ell \neq 0$. If $K_f \neq \mathbb{Q}$ then there is a positive density of primes $\ell$ such that $c_\ell \notin \mathbb{Q}$ and choosing any of these with $\ell \nmid 2L$ gives a bound for $p$, and we

will be content with that. From now on our aim is to show that $p$ is bounded. For example, there are newforms of weight 2 and level $2 \times 37$ but these are irrational (a newform $f$ is **irrational** if $K_f \neq \mathbb{Q}$ and **rational** if $K_f = \mathbb{Q}$). Thus the exponent $p$ is bounded for non-trivial solutions to (2.1) when $L = 37$. However, this is not the case for $L = 7, 13, 17, 19, 23, 29, 31, 41, \ldots$ where we do find rational newforms at levels $2L$. We now ignore the irrational newforms (as they give a bound for $p$) and focus on the rational ones.

A theorem of Eichler and Shimura asserts that a rational weight 2 newform $f$ corresponds to an isogeny class of elliptic curves $E$ defined over $\mathbb{Q}$. This correspondence was made more precise by Carayol [Car83] who showed that the level $N$ of $f$ is equal to the conductor of each $E$ in the isogeny class. The correspondence asserts that $a_\ell(E) = c_\ell$ for all primes $\ell \nmid N$. We apply this to our rational newform $f$ of weight 2 and level $N = 2L$. The earlier congruences become

$$\begin{cases} a_\ell(E') \equiv a_\ell(E) \pmod{p} & \text{if } \ell \nmid xyz \\ \pm(\ell+1) \equiv a_\ell(E) \pmod{p} & \text{if } \ell \mid xyz. \end{cases}$$

Note that $E'$ has full 2-torsion and thus $4 \mid \#E'(\mathbb{F}_\ell)$ for all primes $\ell$ of good reduction. However, $\#E'(\mathbb{F}_\ell) = \ell + 1 - a_\ell(E')$. Thus $a_\ell(E')$ belongs to the set

$$T_\ell = \{a \in \mathbb{Z} \, : \, -2\sqrt{\ell} \leq a \leq 2\sqrt{\ell}, \qquad \ell + 1 \equiv a \pmod{4}\}.$$

This leads us to conclude that $p$ divides

$$\gamma_\ell := \ell \cdot (\ell + 1 - a_\ell(E)) \cdot (\ell + 1 + a_\ell(E)) \cdot \prod_{a \in T_\ell} (a - a_\ell(E))$$

for any prime $\ell \nmid 2L$. If $\gamma_\ell$ is non-zero for some $\ell \nmid 2L$ then we have a bound for the exponent $p$ for non-trivial solutions to (2.1). If $a_\ell(E) \notin T_\ell$ for some prime $\ell \nmid 2L$ then $\gamma_\ell$ is non-zero and we have a bound for $p$. Thus we are reduced to the case where $a_\ell(E) \in T_\ell$ or equivalently $4 \mid \#E(\mathbb{F}_\ell)$, for all primes $\ell \nmid 2L$. In that case, it follows from [ŞS18, Lemma 7.5] that $E$ is isogenous to an elliptic curve with full 2-torsion, and since $E$ is really determined only up to isogeny we now suppose that $E$ has full 2-torsion. It remains to determine, for which odd primes $L$, there is an elliptic curve $E/\mathbb{Q}$ with full 2-torsion and conductor $2L$. The answer is given by the following lemma.

**Lemma 2.1.** *Let $L$ be an odd prime. Then there is an elliptic curve $E/\mathbb{Q}$ with full 2-torsion and conductor $2L$ if and only if $L$ is a Mersenne or a Fermat prime and $L \geq 31$.*

*Proof.* Such an $E$ necessarily has model

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

with $a$, $b \in \mathbb{Z}$ and $ab(a+b) \neq 0$; indeed the discriminant is $16a^2b^2(a+b)^2$. Moreover we can choose $a$, $b$ so that this model is minimal away from 2. Thus

$$a^2b^2(a+b)^2 = 2^u L^v$$

for some non-negative integers $u$, $v$. It follows that

$$a = \pm 2^{u_1} L^{v_1}, \qquad b = \pm 2^{u_2} L^{v_2}, \qquad a + b = \pm 2^{u_3} L^{v_3}.$$

Thus

$$\pm 2^{u_1} L^{v_1} \pm 2^{u_2} L^{v_2} = \pm 2^{u_3} L^{v_3}. \tag{2.2}$$

This is an $S$-unit equation with $S = \{2, L\}$ ($S$-unit equations are defined in Section 4). It is an easy exercise to conclude from this equation that $L$ is a Fermat or a Mersenne prime, or that $v_1 = v_2 = v_3$. However if $v_1 = v_2 = v_3$ then the exponent of $L$ in the conductor of $E$ is not 1. Also for the Mersenne and Fermat primes $L = 3$, 5, 7 and 17, the exponent of 2 in the conductor of $E$ is not 1. So we conclude that $L$ is a Mersenne or a Fermat prime and $L \geq 31$. □

We have the following theorem.

**Theorem 2.2** (Serre and Mazur)**.** *Let $L$ be an odd prime. Suppose $L < 31$, or $L$ is neither a Mersenne nor a Fermat prime. Then there is a constant $C_L$ such that for all primes $p > C_L$ the only solutions $(x, y, z) \in \mathbb{Z}^3$ to the equation* (2.1) *are the trivial ones satisfying $xyz = 0$.*

We note in passing that the equation $x^p + y^p + 2^r z^p = 0$ is much more difficult due to the presence of the non-trivial solution $(x, y, z, r) = (1, 1, -1, 1)$ for all exponents $p$. Thus no bound for the exponents $p$ of non-trivial solutions is possible. Ribet [Rib97] and Darmon and Merel [DM97] showed that there are no solutions apart from the trivial ones and $(x, y, z, r) = (1, 1, -1, 1)$ and $(-1, -1, 1, 1)$.

## 3. Modular Approach—A General Sketch

Most modern attacks on Fermat-type equations (1.2) over a number field $K$ follow the strategy of Serre and Mazur outlined in the previous section, which we now briefly describe in more generality. Again the reader should feel free to skim this section. The steps are roughly as follows:

(I) Associate a Frey elliptic curve $E'$ to a non-trivial solution $(x, y, z)$.

(II) Show that the mod $p$ representation $\overline{\rho}_{E',p}$ is irreducible. No generalization of Mazur's isogeny theorem is available over number fields. However the desired irreducibility often follows for suitably large $p$ from Merel's uniform boundedness theorem using the fact that the Frey curve is close to being semistable. This approach is explained in [FS15b].

(III) Show that the $\overline{\rho}_{E',p}$ is modular of parallel weight 2 and level $\mathcal{N}$ which is independent of the solution $(x, y, z)$ (the level $\mathcal{N}$ is an ideal of the ring of integers $\mathcal{O}_K$). Over totally real fields it is often possible to use the work of Kisin, Gee, and others to achieve this. For example, in [FLHS15] it is shown that for a given totally real field $K$ all but finitely many $j$-invariants are modular. This is usually enough to show that $\overline{\rho}_{E',p}$ is modular for $p$ sufficiently large. Over general number fields we know much less about modularity of elliptic curves and it is often necessary to assume a version of Serre's modularity conjecture, as for example in [ŞS18], [Ţur18].

(IV) Determine newforms of parallel weight 2 and level $\mathcal{N}$. This is often a difficult step over number fields. If there are none then one can conclude that there are no non-trivial solutions. If they are all irrational then one should be able to at least bound the exponent $p$.

(V) Instead of determining all newforms of parallel weight 2 and level $\mathcal{N}$ one can focus on the rational newforms. Here there is a conjectural generalization of the Eichler–Shimura theorem which is often called the Eichler–Shimura conjecture. If $K$ is totally real this simply says that a newform of parallel weight 2 and level $\mathcal{N}$ corresponds to an isogeny class of elliptic curves $E$ of conductor $\mathcal{N}$, and this conjecture is in fact known to be true (e.g. [Hid81])

if $\mathcal{N}$ is not squarefull (i.e. there is a prime ideal $\mathfrak{q}$ with $\mathrm{ord}_{\mathfrak{q}}(\mathcal{N}) = 1$). For a version of the Eichler–Shimura conjecture over general number fields $K$ see [ŞS18]. At any rate, assuming this conjecture, or relying on special cases of the conjecture that are theorems, we know the existence of an elliptic curve $E/K$ of conductor $\mathcal{N}$ with $\overline{\rho}_{E',p} \sim \overline{\rho}_{E,p}$. It is usually possible to show that $E$ has the same torsion structure as $E'$.

(VI) So we would like to determine all elliptic curves $E/K$ of condutor $\mathcal{N}$ and having a certain torsion structure. This can be treated as a Diophantine problem. For example, to determine all elliptic curves $E/K$ of conductor $\mathcal{N}$ with full 2-torsion it is enough to solve a certain $S$-unit equation where $S$ is the set of prime ideals dividing $2\mathcal{N}$ (we will say more on that in Section 5). Not every solution to the $S$-unit equation will lead back to an elliptic curve of the right conductor. For example, in the proof of Lemma 2.1 we excluded solutions to the $S$-unit equation (2.2) with $v_1 = v_2 = v_3$ as these do not lead back to an elliptic curve of conductor $2L$. Thus we are probably interested in all solutions to the $S$-unit equation that satisfy further restrictive conditions.

## 4. $S$-Unit Equations

Let $K$ be a number field, $\mathcal{O}_K$ be its ring of integers and $S$ be a finite set of primes ideals of $\mathcal{O}_K$. In simplest terms, the notion of $S$-unit generalizes the idea of a unit in $\mathcal{O}_K$.

**Definition 4.1.** *An $S$-**unit** is an element $\alpha$ in $K$ such that the principal fractional ideal generated by $\alpha$ can be written as a product of the prime ideals in $S$. In other words, the set of $S$-units $\mathcal{O}_S^*$ can be defined as:*

$$\mathcal{O}_S^* = \{\alpha \in K^* \ : \ \mathrm{ord}_{\mathfrak{p}}(\alpha) = 0 \quad \textit{for all } \mathfrak{p} \notin S\}.$$

*Similarly the set of $S$-integers in $K$ is*

$$\mathcal{O}_S = \{\alpha \in K^* \ : \ \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0 \quad \textit{for all } \mathfrak{p} \notin S\}.$$

Note that $S$-units $\mathcal{O}_S^*$ are units of the ring of $S$-integers $\mathcal{O}_S$.

**Example 4.2.** Let $K = \mathbb{Q}$. Every ideal of $\mathcal{O}_K = \mathbb{Z}$ is principal, and prime ideals are generated by primes. Thus we may think of $S$ as a finite set of primes $S = \{p_1, p_2, \ldots, p_r\}$. Then an $S$-unit of $K$ is a rational number $\frac{a}{b}$ such that $a$ and $b$ are only divisible by the primes in $S$; i.e.

$$\mathcal{O}_S^* = \{\pm p_1^{a_1} \cdots p_r^{a_r} \ : \ a_1, \ldots, a_r \in \mathbb{Z}\}.$$

**Example 4.3.** Let $K = \mathbb{Q}(\sqrt{5})$, whence $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

- If $S = \emptyset$ then $\mathcal{O}_S^* = \left\{\pm\left(\frac{1+\sqrt{5}}{2}\right)^r : r \in \mathbb{Z}\right\}$.
- If $S = \{2\mathcal{O}_K\}$ then $\mathcal{O}_S^* = \left\{\pm 2^r \left(\frac{1+\sqrt{5}}{2}\right)^s : r,\ s \in \mathbb{Z}\right\}$.

If $S$ and $T$ are sets of prime ideals and $T \subseteq S$ then $\mathcal{O}_T^*$ is a subgroup of $\mathcal{O}_S^*$. Observe that the unit group $\mathcal{O}_K^*$ is precisely $\mathcal{O}_\emptyset^*$. Thus $\mathcal{O}_K^*$ is a subgroup of $\mathcal{O}_S^*$, and every unit is indeed an $S$-unit. Many facts concerning units have generalizations to $S$-units.

**Theorem 4.4** (Dirichet's $S$-Unit Theorem)**.** *The $S$-unit group $\mathcal{O}_S^*$ is finitely generated with rank equal to $r_1 + r_2 + \#S - 1$, where $(r_1, r_2)$ is the signature of $K$.*

Observe that letting $S = \emptyset$ allows us to see the Dirichlet's unit theorem as a special case of Dirichlet's $S$-unit theorem.

**Definition 4.5.** *Let $K$ be a number field and $S$ a finite set of prime ideals of $\mathcal{O}_K$. The **$S$-unit equation** is the equation*

$$\lambda + \mu = 1, \qquad \lambda,\ \mu \in \mathcal{O}_S^*. \tag{4.1}$$

*If $S = \emptyset$ so $\mathcal{O}_S^* = \mathcal{O}_K^*$ then this is called the **unit equation**.*

**Theorem 4.6** (Siegel 1921, Parry 1950)**.** *Let $K$ be a number field and $S$ a finite set of prime ideals of $\mathcal{O}_K$. The $S$-unit equation* (4.1) *has only finitely many solutions.*

The original proofs due to Siegel and Parry are non-effective. Later on, Baker's theory of linear forms in logarithms gave effective though very large bounds for the solutions. In his 1989 PhD thesis Benne de Weger [dW89] showed how these bounds can be combined with the LLL algorithm to give a practical method for solving such equations. Variants of de Weger's algorithm can be found in Smart's book [Sma98] and also in [AKM$^+$19] and [KM16].

**Example 4.7.** We illustrate the practicality of the algorithm of de Weger and its variants through the following example. Let $F = \mathbb{Q}(\zeta_{16})$ where $\zeta_{16}$ is a primitive 16-th root of unity. Then $F$ is a totally complex number field of degree 8. Let $\mathfrak{p} = (1 - \zeta_{16}) \cdot \mathcal{O}_F$; this is the unique prime above 2. Let $S' = \{\mathfrak{p}\}$. Smart [Sma99] determines the solutions to the equation $\lambda + \mu = 1$ with $\lambda,\ \mu \in \mathcal{O}_{S'}^*$ and finds that there are precisely 795 solutions $(\lambda, \mu)$—too many to enumerate here!

Let $K = F^+ = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1}) = \mathbb{Q}\left(\sqrt{2 + \sqrt{2}}\right)$ be the maximal totally real subfield of $F$, which has degree 4. Let $\mathfrak{P} = \sqrt{2 + \sqrt{2}} \cdot \mathcal{O}_K$ be the unique prime above 2 in $\mathcal{O}_K$, and let $S = \{\mathfrak{P}\}$. The $S$-unit equation $\lambda + \mu = 1$ with $\lambda,\ \mu \in \mathcal{O}_S^*$ has 585 solutions. Of course this is a subset of the 795 solutions to the $S'$-unit equation in $F$.

**Example 4.8.** Let $K$ be a number field in which there is a degree 1 prime $\mathfrak{P}$ above 2 (i.e. the residue field $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$). Let $S$ be a finite set of prime ideals of odd norm. If $\lambda,\ \mu \in \mathcal{O}_S^*$ then $\lambda,\ \mu \equiv 1 \pmod{\mathfrak{P}}$ and so $\lambda + \mu \equiv 0 \pmod{\mathfrak{P}}$. Thus the $S$-unit equation (4.1) has no solutions.

Before de Weger the most promising method for solving $S$-unit equations was Skolem's $p$-adic method (now often called Chabauty–Coleman–Skolem). This method still has a lot of promise, as the following recent and beautiful theorem of Nicholas Triantafillou [Tri20b] shows.

**Theorem 4.9** (Triantafillou)**.** *Let $K$ be a number field. Suppose that $3 \nmid [K : \mathbb{Q}]$ and 3 splits completely in $K$. Then there is no solution to the unit equation in $K$. In other words, there is no pair $\lambda,\ \mu \in \mathcal{O}_K^*$ such that $\lambda + \mu = 1$.*

*Proof.* We can't resist giving an exposition of Triantafillou's elegant argument. Let $K$ be a number field in which 3 splits completely, and write $3\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ where $n = [K : \mathbb{Q}]$ and the $\mathfrak{p}_j$ are distinct prime ideals with residue field $\mathbb{F}_3$. Let $\theta \in \mathcal{O}_K^*$. Then $\theta \equiv \pm 1 \pmod{\mathfrak{p}_j}$ and hence $\theta^2 \equiv 1 \pmod{\mathfrak{p}_j}$ for all $j$. Thus $\theta^2 \equiv 1 \pmod{3\mathcal{O}_K}$.

Now let $\lambda,\ \mu \in \mathcal{O}_K^*$ satisfy $\lambda + \mu = 1$. By the above

$$\lambda^2 \equiv 1 \pmod{3\mathcal{O}_K}, \qquad (\lambda - 1)^2 = (-\mu)^2 \equiv 1 \pmod{3\mathcal{O}_K}.$$

Hence $2\lambda - 1 = \lambda^2 - (\lambda - 1)^2 \equiv 0 \pmod{3\mathcal{O}_K}$, so $\lambda \equiv -1 \pmod{3\mathcal{O}_K}$. We write $\lambda = -1 + 3\phi$ with $\phi \in \mathcal{O}_K$. Let $\phi_1, \ldots, \phi_n$ be the images of $\phi$ under the $n$ embeddings $K \hookrightarrow \overline{\mathbb{Q}}$. As $\lambda$ is a unit

$$\pm 1 = \mathrm{Norm}(\lambda) = (-1+3\phi_1)\cdots(-1+3\phi_n) \equiv (-1)^n + (-1)^{n-1} \cdot 3\,\mathrm{Tr}(\phi) \pmod 9.$$

By considering all the choices for $\pm 1$ and $(-1)^n$, we obtain $3\,\mathrm{Tr}(\phi) \equiv -2$, 2 or 0 (mod 9). The first two are plainly impossible and so $\mathrm{Tr}(\phi) \equiv 0 \pmod 3$.

However $\mu = 1 - \lambda = 2 - 3\phi = -1 + 3(1-\phi)$ is also a unit. Thus by the above, $\mathrm{Tr}(1-\phi) \equiv 0 \pmod 3$. But $\mathrm{Tr}(1-\phi) = n - \mathrm{Tr}(\phi)$. Therefore $n \equiv 0 \pmod 3$ completing the proof. □

Perhaps the most elegant theorem on $S$-unit equations is the following result due to Evertse [Eve84].

**Theorem 4.10** (Evertse)**.** *Let $(r_1, r_2)$ be the signature of $K$ and let $S$ be a finite set of prime ideals of $\mathcal{O}_K$. Then the $S$-unit equation* (4.1) *has at most $3 \times 7^{3r_1+4r_2+2\#S}$ solutions.*

For extensive surveys of results on $S$-unit equations, see [EG15] and the introduction of [BB17]. Nowadays the $S$-unit equation is often viewed as $S$-integral points on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, allowing for a variety of high-powered approaches from arithmetic geometry to be applied, e.g. [Kim05], [LV18], [Tri20a].

## 5. S-Unit Equations and Elliptic Curves

In this section we explore more fully the relationship between solutions to $S$-unit equations and certain families of elliptic curves. A theorem of Shafarevich asserts that given a finite set of prime ideals $S$ in the ring of integers $\mathcal{O}_K$ of a number field $K$, there are only finitely many elliptic curves $E/K$ with good reduction outside $S$. For illustration we consider a special case of this problem where $K = \mathbb{Q}$ and $E$ is assumed to have a point of order 2. There is no loss of generality in supposing that $2 \in S$. We write $S = \{2, p_1, p_2, \ldots, p_k\}$ where $p_1, \ldots, p_k$ are distinct odd primes. We may suppose that $E$ has a model of the form

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

where $a$, $b$ are rational integers, and the discriminant $\Delta = 16b^2(a^2 - 4b) \neq 0$. Moreover, we can choose $a$, $b$ so that this model is minimal away from 2. As $E$ has good reduction away from $S$ we see that

$$b^2(a^2 - 4b) = \pm 2^{\alpha_0} p_1^{\alpha_1} \ldots p_k^{\alpha_k}$$

where $\alpha_i$ are nonnegative integers. Then

$$b = \pm 2^{\beta_0} p_1^{\beta_1} \ldots p_k^{\beta_k}, \qquad a^2 - 4b = \pm 2^{\alpha_0 - 2\beta_0} p_1^{\alpha_1 - 2\beta_1} p_2^{\alpha_2 - 2\beta_2} \ldots p_k^{\alpha_k - 2\beta_k}$$

for some integers $0 \leq \beta_i \leq \alpha_i$. Note that this gives a solution to the equation $x + y = z^2$ with

$$\begin{cases} x = \pm 2^{\alpha_0 - 2\beta_0} p_1^{\alpha_1 - 2\beta_1} p_2^{\alpha_2 - 2\beta_2} \ldots p_k^{\alpha_k - 2\beta_k} \in \mathcal{O}_S^*, \\ y = 4b = \pm 2^{\beta_0 + 2} p_1^{\beta_1} \ldots p_k^{\beta_k} \in \mathcal{O}_S^*, \\ z = a \in \mathbb{Z}. \end{cases}$$

More generally the task of determining elliptic curves with a point of order 2 over a number field $K$ and a good reduction outside a finite set of prime ideals $T$ reduces to solving an equation of the form

$$x + y = z^2, \qquad x,\ y \in \mathcal{O}_S^*, \qquad z \in K \tag{5.1}$$

where $S$ is a suitable enlargement of $T$ that takes account of the class group of $K$. An algorithm for solving equations of the form (5.1) is given in de Weger's thesis [dW89]. See also [BGR19].

We now look at a similar problem that arises in the context of understanding Fermat-type equations over number fields. Let $K$ be a number field. An elliptic curve $E/K$ is said to have **potentially good reduction** at a prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$ if there is a finite extension $L/K$ so that $E/L$ has good reduction at every prime ideal $\mathfrak{q}'$ of $\mathcal{O}_L$ above $\mathfrak{q}$. It is possible to show that $E/K$ has potentially good reduction at $\mathfrak{q}$ if and only if $\mathrm{ord}_{\mathfrak{q}}(j(E)) \geq 0$ where $j(E)$ is the $j$-invariant of $E$. Now let $S$ be a finite set of prime ideals of $\mathcal{O}_K$. We are interested in the set $\mathcal{E}_S$ of elliptic curves $E/K$ with full 2-torsion and potentially good reduction outside $S$. Here we suppose that $S$ includes all the prime ideals of $\mathcal{O}_K$ above 2. We follow the treatment in [Dec16]. By assumption the elliptic curves we are dealing with are of the form

$$E\ :\ Y^2 = (X - a_1)(X - a_2)(X - a_3) \tag{5.2}$$

where the $a_i \in K$ are distinct. Let $\lambda = (a_3 - a_1)/(a_2 - a_1) \in \mathbb{P}^1(K) - \{0, 1, \infty\}$. This is called the **$\lambda$-invariant** of $E$.

**Lemma 5.1.** *Let $\mathcal{S}_3$ be the symmetric group on three elements. The action of $\mathcal{S}_3$ on $\{a_1, a_2, a_3\}$ can be extended to $\mathbb{P}^1(K) - \{0, 1, \infty\}$. Under this action the orbit of $\lambda = (a_3 - a_1)/(a_2 - a_1) \in \mathbb{P}^1(K) - \{0, 1, \infty\}$ is*

$$\left\{\lambda,\ \frac{1}{\lambda},\ 1 - \lambda,\ \frac{1}{(1-\lambda)},\ \frac{\lambda}{(\lambda - 1)},\ \frac{(\lambda - 1)}{\lambda}\right\}. \tag{5.3}$$

*Proof.* This is a straightforward computation. For example if $\sigma \in \mathcal{S}_3$ is the transposition $(1, 2)$ then it swaps $a_1$, $a_2$ and keeps $a_3$ fixed. Hence

$$\sigma(\lambda) = (a_3 - a_2)/(a_1 - a_2) = 1 - \lambda.$$

□

From now on we think of $\mathcal{S}_3$ as acting on $\mathbb{P}^1(K) - \{0, 1, \infty\}$, via the six transformations $\lambda \mapsto \lambda$, $\lambda \mapsto 1/\lambda$, $\lambda \mapsto 1 - \lambda$, ...

**Lemma 5.2.** *The set of $\lambda$-invariants $\mathbb{P}^1(K) - \{0, 1, \infty\}$, up to equivalence under the action of $\mathcal{S}_3$, is in one to one correspondence with the set of elliptic curves over $K$ with full two torsion up to isomorphism over $\overline{K}$.*

*Proof.* This is essentially Proposition III.1.7 in Silverman's book [Sil09]. The correspondence is induced by the association $E \mapsto \lambda = (a_3 - a_1)/(a_2 - a_1)$ where $E$ has the form (5.2). The inverse is given by sending the class of $\lambda \in \mathbb{P}^1(K) - \{0, 1, \infty\}$ to the $\overline{K}$-isomorphism class of the Legendre elliptic curve

$$E_\lambda\ :\ Y^2 = X(X - 1)(X - \lambda).$$

□

Let

$$W_S = \{(\lambda, \mu) : \lambda + \mu = 1, \lambda, \mu \in \mathcal{O}_S^*\}$$

be the set of solutions of the $S$-unit equation (4.1). Recall that $\mathcal{E}_S$ is the set of elliptic curves over $K$ with full 2-torsion and having potentially good reduction outside $S$. If $E_1, E_2$ are in $\mathcal{E}_S$ and isomorphic over the algebraic closure of $K$ then we say that $E_1, E_2$ are **equivalent**.

**Lemma 5.3.** *Suppose $S$ is a finite set of prime ideals of $\mathcal{O}_K$ that includes all the primes above 2. Then $\mathcal{S}_3$ acts on $W_S$ via $\pi(\lambda, \mu) = (\pi(\lambda), 1 - \pi(\lambda))$; here $\pi(\lambda)$ denotes the image of $\lambda$ under $\pi$ as in Lemma 5.1. Moreover the $\mathcal{S}_3$-orbits in $W_S$ are in bijection with the equivalence classes in $\mathcal{E}_S$.*

*Proof.* This is essentially routine computation; for full details see [Dec16, Section 5]. The bijection is induced by the maps in Lemma 5.2. □

## 6. $S$-Unit Equations and Fermat

In this section we state a theorem that relates the Fermat equation over totally real fields to $S$-unit equations, following [FS15a]. Generalizations to fields with complex embeddings are known and we discuss them in later sections, but the statement is easier in the totally real setting. In some cases we will need the Eichler–Shimura conjecture which we now state.

**Conjecture 6.1** ("Eichler–Shimura")**.** *Let $K$ be a totally real field. Let $\mathfrak{f}$ be a Hilbert newform over $K$ of level $\mathcal{N}$ and parallel weight 2, and rational Hecke eigenvalues. Then there is an elliptic curve $E_{\mathfrak{f}}/K$ with conductor $\mathcal{N}$ having the same* L*-function as $\mathfrak{f}$.*

Let $K$ be a totally real field, and let

$$S = \{\mathfrak{P} \ : \ \mathfrak{P} \text{ is a prime ideal of } \mathcal{O}_K \text{ above } 2\},$$
$$T = \{\mathfrak{P} \in S \ : \ f(\mathfrak{P}/2) = 1\}, \qquad U = \{\mathfrak{P} \in S \ : \ 3 \nmid \mathrm{ord}_{\mathfrak{P}}(2)\}. \tag{6.1}$$

Here $f(\mathfrak{P}/2)$ denotes the residual degree of $\mathfrak{P}$. We need an assumption, which we refer to as (ES):

$$\textbf{(ES)} \qquad \begin{cases} \text{either } [K : \mathbb{Q}] \text{ is odd;} \\ \text{or } T \neq \emptyset; \\ \text{or Conjecture 6.1 holds for } K. \end{cases}$$

**Theorem 6.2** (Freitas and Siksek)**.** *Let $K$ be a totally real field satisfying (ES). Let $S$, $T$ and $U$ be as in* (6.1)*. Write $\mathcal{O}_S^*$ for the group of $S$-units of $K$. Suppose that for every solution $(\lambda, \mu)$ to the $S$-unit equation* (4.1) *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 Fermat conjecture holds over $K$.*

*Proof Sketch.* The proof largely follows the strategy sketched in Sections 2 and 3. Write $E$ for the Frey curve associated to a non-trivial solution to the generalized Fermat equation (1.1). The strategy relates $\overline{\rho}_{E,p}$ to $\overline{\rho}_{F,p}$ where $F$ is an elliptic curve defined over $K$ with full 2-torsion and conductor $\mathcal{N}$ which does not depend on the solution to the Fermat equation but only on the field $K$. Inspired by ideas of Kraus [Kra98], and of Bennett and Skinner [BS04], Freitas and Siksek study

the possibilities for the image of inertia $\overline{\rho}_{E,p}(I_{\mathfrak{P}})$. Since the representations $\overline{\rho}_{E,p}$ and $\overline{\rho}_{F,p}$ are isomorphic this yields information about the elliptic curve $F$. In particular they deduce that $F$ has potentially good reduction at all primes outside $S$. Lemma 5.3 relates $F$ to a solution $(\lambda, \mu)$ of the $S$-unit equation (4.1). The theorem follows from examining the possibilities for $\overline{\rho}_{E,p}(I_{\mathfrak{P}})$ and $\overline{\rho}_{F,p}(I_{\mathfrak{P}})$ at the primes $\mathfrak{P} \in T$, $U$ and relating these to the solution $(\lambda, \mu)$ of the $S$-unit equation (4.1) corresponding to $F$. If either of hypotheses (A), (B) of the theorem is satisfied then there will exist a prime $\mathfrak{P}$ such that $\overline{\rho}_{E,p}(I_{\mathfrak{P}}) \ncong \overline{\rho}_{F,p}(I_{\mathfrak{P}})$, and therefore the representations $\overline{\rho}_{E,p}$ and $\overline{\rho}_{F,p}$ are non-isomorphic, giving a contradiction. □

We point out that a generalization of Theorem 6.2 to general number fields is given by Şengün and Siksek [ŞS18], assuming standard conjectures stated in the following section.

**Example 6.3.** Let $K = \mathbb{Q}(\zeta_{16})^+ = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$. This is a degree 4 totally real field in which 2 is totally ramified: $2\mathcal{O}_K = \mathfrak{P}^4$ where $\mathfrak{P} = \sqrt{2+\sqrt{2}} \cdot \mathcal{O}_K$. In particular, $S = T = \{\mathfrak{P}\}$ in the above notation. As stated in Example 4.7 the $S$-unit equation (4.1) has 585 solutions. It turns out that they all satisfy condition (A) of the theorem. Hence the asymptotic Fermat conjecture holds for $K$.

Through a detailed study of solutions to $S$-unit equations over real quadratic fields, Freitas and Siksek [FS15a] prove the following, which in essence says that the asymptotic Fermat conjecture holds for almost all real quadratic fields.

**Theorem 6.4** (Freitas and Siksek)**.** *Let $\mathbb{N}^{\mathrm{sf}}$ denote the set of squarefree natural numbers $> 1$. Let $\mathcal{F}$ be the subset of $d \in \mathbb{N}^{\mathrm{sf}}$ for which the asymptotic Fermat conjecture holds over $\mathbb{Q}(\sqrt{d})$. Then*

$$\liminf_{X\to\infty} \frac{\#\{d \in \mathcal{F} \,:\, d \le X\}}{\#\{d \in \mathbb{N}^{\mathrm{sf}} \,:\, d \le X\}} \ge 5/6.$$

*If we assume the Eichler–Shimura conjecture then*

$$\lim_{X\to\infty} \frac{\#\{d \in \mathcal{F} \,:\, d \le X\}}{\#\{d \in \mathbb{N}^{\mathrm{sf}} \,:\, d \le X\}} = 1.$$

6.1. **$S$-Unit Equations and $\mathbb{Z}_\ell$-Layers.** In two recent works [FKS20a] and [FKS20b], Freitas, Kraus and Siksek prove the asymptotic Fermat conjecture for the layers of various cyclotomic $\mathbb{Z}_\ell$-extensions of $\mathbb{Q}$. We first introduce these extensions. Let $\ell$ be a rational prime. For now let $\ell$ be odd and $n \ge 1$. The cyclotomic field $\mathbb{Q}(\zeta_{\ell^{n+1}})$ has a unique subfield of degree $\ell^n$ which we denote by $\mathbb{Q}_{n,\ell}$. This is a cyclic, totally real extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}/\ell^n\mathbb{Z}$. Clearly $\mathbb{Q}_{n,\ell}$ is a subfield of $\mathbb{Q}_{n+1,\ell}$. The union of these fields is denoted

$$\mathbb{Q}_{\infty,\ell} = \bigcup_{n=1}^{\infty} \mathbb{Q}_{n,\ell}$$

and has Galois group isomorphic to $\mathbb{Z}_\ell$. This is called the cyclotomic $\mathbb{Z}_\ell$-extension of $\mathbb{Q}$, and the field $\mathbb{Q}_{n,\ell}$ is called the $n$-th layer of $\mathbb{Q}_{\infty,\ell}$.

For $\ell = 2$ all the above is true with a small adjustment: we take $\mathbb{Q}_{n,2} = \mathbb{Q}(\zeta_{2^{n+2}})^+$. In [FKS20a] the following theorem is proven.

**Theorem 6.5.** *The asymptotic Fermat conjecture is true for $\mathbb{Q}_{n,2}$.*

*Proof Sketch.* Write $K = \mathbb{Q}_{n,2}$. Then 2 is totally ramified in $\mathcal{O}_K$ and we let $\mathfrak{P}$ be the unique prime above 2. In the notation of Theorem 6.2, $S = T = \{\mathfrak{P}\}$. The key to the proof is to show that every solution $(\lambda, \mu)$ to the $S$-unit equation (4.1) satisfies condition (A) of Theorem 6.2. Let $(\lambda, \mu)$ be a solution (4.1). Write

$$m_{\lambda,\mu} := \max\{|\mathrm{ord}_{\mathfrak{P}}(\lambda)|, |\mathrm{ord}_{\mathfrak{P}}(\mu)|\};$$

this is the quantity appearing in criterion (A) of Theorem 6.2. Suppose

$$m_{\lambda,\mu} > 2\,\mathrm{ord}_{\mathfrak{P}}(2). \tag{6.2}$$

The $\mathcal{S}_3$-action does not affect the value of $m_{\lambda,\mu}$, and by considering this action on $(\lambda, \mu)$ we may suppose that $\mathrm{ord}_{\mathfrak{P}}(\mu) = 0$ and $\mathrm{ord}_{\mathfrak{P}}(\lambda) = m_{\lambda,\mu}$. Then $\mu \in \mathcal{O}_K^*$ and $\mu = 1 - \lambda \equiv 1 \pmod 4$ by assumption (6.2). It follows from this that the extension $K(\sqrt{\mu})/K$ is unramified at $\mathfrak{P}$. Since $\mu$ is a unit, this extension is unramified at all odd primes. Thus $K(\sqrt{\mu})/K$ is unramified at all the finite places. We now shall need a theorem due to Iwasawa which asserts that $K = \mathbb{Q}_{n,2}$ has odd narrow class number. Thus $K(\sqrt{\mu}) = K$ and so $\mu$ is a square. We write $\mu = \delta^2$ where $\delta \in \mathcal{O}_K^*$. Thus

$$(1 + \delta)(1 - \delta) = 1 - \mu = \lambda.$$

Hence

$$\lambda = \lambda_1\lambda_2, \qquad \lambda_1 = 1 + \delta, \qquad \lambda_2 = 1 - \delta.$$

Now

$$\lambda_1 + \lambda_2 = 2, \qquad \lambda_1 - \lambda_2 = 2\delta. \tag{6.3}$$

It follows easily that one of the $\mathrm{ord}_{\mathfrak{P}}(\lambda_i)$ is $m - \mathrm{ord}_{\mathfrak{P}}(2)$ and the other is $\mathrm{ord}_{\mathfrak{P}}(2)$, where $m = m_{\lambda,\mu} = \mathrm{ord}_{\mathfrak{P}}(\lambda)$. By swapping $\delta$ and $-\delta$ if necessary, we may suppose $\mathrm{ord}_{\mathfrak{P}}(\lambda_1) = m - \mathrm{ord}_{\mathfrak{P}}(2)$ and $\mathrm{ord}_{\mathfrak{P}}(\lambda_2) = \mathrm{ord}_{\mathfrak{P}}(2)$. Multiplying the two equations in (6.3), dividing by $\lambda_2^2$ and rearranging we obtain

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

Observe that $\lambda'$, $\mu' \in \mathcal{O}_S^*$ so we obtain another solution to (4.1). Moreover,

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

where the last inequality follows from (6.2). This shows that the solution $(\lambda', \mu')$ is different from $(\lambda, \mu)$ and also satisfies (6.2). Repeating the argument allows us to construct infinitely many solutions to the $S$-unit equation contradicting Siegel's theorem (Theorem 4.6). Thus assumption 6.2 is false. We deduce that every solution to (4.1) satisfies $m_{\lambda,\mu} \leq 2\,\mathrm{ord}_{\mathfrak{P}}(2)$ and in particular satisfies condition (A) of Theorem 6.2. This completes the proof. □

The following more recent theorem is from [FKS20b].

**Theorem 6.6** (Freitas, Kraus and Siksek)**.** *Let $\ell \geq 5$ be an odd prime. Suppose $\ell$ is non-Wieferich (i.e. $2^{\ell-1} \not\equiv 1 \pmod{\ell^2}$). Then the asymptotic Fermat conjecture holds over $\mathbb{Q}_{n,\ell}$ for all $n \geq 1$.*

A key step towards the proof of this theorem is the following theorem about unit equations, which applies to $K = \mathbb{Q}_{n,\ell}$ with $\ell \geq 5$.

**Theorem 6.7.** *Let $\ell \geq 5$ be an odd prime. Let $K$ be an $\ell$-extension of $\mathbb{Q}$ (i.e. a finite Galois extension of $\mathbb{Q}$ with degree $[K : \mathbb{Q}] = \ell^n$ for some $n \geq 1$). Suppose $\ell$ is totally ramified in $\mathcal{O}_K$. Then there is no solution to the unit equation in $K$.*

*Proof.* Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $\mathfrak{L}$ be the unique prime ideal of $\mathcal{O}_K$ above $\ell$. As $\ell$ is totally ramified in $\mathcal{O}_K$, we know that $\mathfrak{L}^\sigma = \mathfrak{L}$ for all $\sigma \in G$. Moreover, the residue field $\mathcal{O}_K/\mathfrak{L}$ is simply $\mathbb{F}_\ell$. In particular, for any $\lambda \in \mathcal{O}_K$ then there is some $a \in \mathbb{Z}$ such that $\lambda \equiv a \pmod{\mathfrak{L}}$. Applying $\sigma \in G$ to this congruence we see that $\lambda^\sigma \equiv a \pmod{\mathfrak{L}}$. Let Norm denote the norm for the extension $K/\mathbb{Q}$. Then

$$\mathrm{Norm}(\lambda) = \prod_{\sigma \in G} \lambda^\sigma \equiv a^{\#G} \pmod{\mathfrak{L}}.$$

Since $\mathcal{O}_K/\mathfrak{L} = \mathbb{F}_\ell$ and since $\#G = \ell^n$, Fermat's Little Theorem gives $a^{\#G} \equiv a \equiv \lambda \pmod{\mathfrak{L}}$. We deduce that $\mathrm{Norm}(\lambda) \equiv \lambda \pmod{\mathfrak{L}}$ for all $\lambda \in \mathcal{O}_K$.

Now let $\lambda,\ \mu \in \mathcal{O}_K^*$ and suppose $\lambda + \mu = 1$. By the above $\lambda \equiv \pm 1 \pmod{\mathfrak{L}}$ and $\mu \equiv \pm 1 \pmod{\mathfrak{L}}$. Hence $\pm 1 \pm 1 \equiv 1$ in $\mathcal{O}_K/\mathfrak{L} = \mathbb{F}_\ell$. This is impossible as $\ell \geq 5$. □

## 7. Generalizations

Let $K$ be a number field (we drop the assumption that $K$ is totally real). Let $A$, $B$, $C$ be non-zero elements of $\mathcal{O}_K$. We consider the following generalized Fermat equation

$$Ax^p + By^p + Cz^p = 0, \tag{7.1}$$

and we are interested in solutions $(x, y, z) \in K^3$. We say that such a solution is **trivial** if $xyz = 0$ otherwise we say it is **non-trivial**. We propose the following generalization of the asymptotic Fermat conjecture.

**Conjecture 7.1** (A Generalized Asymptotic Fermat Conjecture)**.** *Let $K$ be a number field, and $A$, $B$, $C$ be non-zero elements of $\mathcal{O}_K$. Let $\Omega$ be the subgroup of roots of unity inside $\mathcal{O}_K^*$. Suppose*

$$A\omega_1 + B\omega_2 + C\omega_3 \neq 0,$$

*for every $\omega_1$, $\omega_2$, $\omega_3 \in \Omega$. Then there exists a constant $\mathcal{B}(K, A, B, C)$ such that for all primes $p > \mathcal{B}(K, A, B, C)$ the only solutions to the Fermat equation* (7.1) *with $(x, y, z) \in K^3$ are the trivial solutions.*

We point out that this conjecture is a straightforward consequence of a suitable version of the $ABC$-conjecture of number fields, such as the one in [Bro06].

Equation (7.1) with $K = \mathbb{Q}$ was first systematically studied using the approach via Galois representations and modular forms by Kraus [Kra97] and by Halberstadt and Kraus [HK02]. In particular, Halberstadt and Kraus proved the following remarkable theorem.

**Theorem 7.2** (Halberstadt and Kraus)**.** *Let $A$, $B$, $C$ be odd rational integers. Then for a positive proportion of primes $p$, the equation* (7.1) *has no non-trivial solutions $(x, y, z) \in \mathbb{Z}^3$.*

More recently, Dieulefait and Soto [DS18] have proved a number of theorems concerning the generalized asymptotic Fermat conjecture, again with $K = \mathbb{Q}$.

**Theorem 7.3** (Dieulefait and Soto)**.** *Let $A$, $B$, $C$ be rational integers divisible only by primes $\equiv 1 \pmod{12}$. Then there is a constant $\mathcal{B}(A, B, C)$ such that if $p > \mathcal{B}(A, B, C)$ then every solution $(x, y, z) \in \mathbb{Z}^3$ to* (7.1) *is trivial.*

Dieulefait and Soto prove their theorems by reducing to $S$-unit equations using the same strategy as explained in Section 2.

Recently a theorem relating the Fermat equation with coefficients $Ax^p + By^p + Cz^p = 0$ over totally real fields to $S$-unit equations was proved by Deconinck [Dec16]. The most general result is due to Kara and Ozman [KO20] which we now describe. Let $K$ be a number field. We assume two standard conjectures from the Langlands programme, which we describe briefly without stating them precisely. For a precise statement of these conjectures see [KO20] or [ŞS18].

(I) Serre's modularity conjecture over $K$. This associates to a totally odd, continuous, finite flat, absolutely irreducible 2 dimensional mod $p$ representation of $\mathrm{Gal}(\overline{K}/K)$ a cuspform of parallel weight 2 whose level is equal to the prime-to-$p$ part of the Artin conductor of the representation.

(II) An "Eichler–Shimura conjecture"over $K$. This associates to a weight 2 cuspform with rational Hecke eigenvalues either an elliptic curve or a "fake elliptic curve". Note that Conjecture 6.1 is a special case of this.

We return to considering (7.1) over a general number field $K$. Let

$$\mathcal{R} = \prod_{\mathfrak{q} \mid ABC} \mathfrak{q}$$

where the product is taken over the prime ideals $\mathfrak{q}$ dividing $ABC$. This is called the **radical** of $ABC$. Let

$$S = \{\mathfrak{P} \ : \ \mathfrak{P} \mid 2\mathcal{R} \text{ is a prime ideal of } \mathcal{O}_K\}.$$

Let

$$T = \{\mathfrak{P} \ : \ \mathfrak{P} \mid 2 \text{ is a prime ideal of } \mathcal{O}_K, \ f(\mathfrak{P}/2) = 1\}.$$

The following is the main theorem of [KO20].

**Theorem 7.4** (Kara and Ozman)**.** *Let $K$ be a number field satisfying conjectures (I) and (II). Let $A$, $B$, $C$ be odd elements of $\mathcal{O}_K$ (i.e. $ABC$ is not divisible by any prime ideal $\mathfrak{P} \mid 2$). Let $S$, $T$ be as above. Suppose that for every solution $(\lambda, \mu)$ to the $S$-unit equation (4.1) there is a prime $\mathfrak{P} \in T$ such that*

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

*Then the Generalized Asymptotic Fermat's Conjecture holds for (7.1); in other words there is a constant $\mathcal{B}(K, A, B, C)$ such that if $p > \mathcal{B}(K, A, B, C)$ is prime then the only solutions to (7.1) are the trivial ones.*

We illustrate the theorem of Kara and Ozman by deriving a slightly stronger version of Theorem 7.3.

**Corollary 7.5.** *Let $\ell$ be an odd prime. Let $A$, $B$, $C$ be rational integers divisible only by primes $\equiv \pm 1 \pmod{4\ell}$. Then there is a constant $\mathcal{B}(A, B, C)$ such that if $p > \mathcal{B}(A, B, C)$ then every solution $(x, y, z) \in \mathbb{Z}^3$ to (7.1) is trivial.*

*Proof.* Serre's modularity conjecture over $\mathbb{Q}$ was proved by Khare and Wintenberger. Over $\mathbb{Q}$ the Eichler–Shimura conjecture is in fact the Eichler–Shimura theorem. Thus we can apply Theorem 7.4 unconditionally. Here, as we're working over $\mathbb{Z}$ we might as well identify prime ideals with primes. Then

$$S = \{2\} \cup \{q_1, q_2, \ldots, q_r\}, \qquad T = \{2\},$$

where the $q_i$ are the prime divisors of $ABC$. Thus $q_i \equiv \pm 1 \pmod{4\ell}$ for $i = 1, \dots, r$. Let $(\lambda, \mu)$ be a solution to the $S$-unit equation $\lambda + \mu = 1$. To deduce the corollary from Theorem 7.4 all we have to do is to show that

$$|\mathrm{ord}_2(\lambda)| \le 4, \qquad |\mathrm{ord}_2(\mu)| \le 4. \tag{7.2}$$

We can rewrite $\lambda + \mu = 1$ as

$$u + v = w, \qquad \lambda = \frac{u}{w}, \qquad \mu = \frac{v}{w},$$

where

$$u = \pm 2^a \cdot q_1^{\alpha_1} \cdots q_r^{\alpha_r}, \qquad v = \pm 2^b \cdot q_1^{\beta_1} \cdots q_r^{\beta_r}, \qquad w = 2^c \cdot q_1^{\beta_1} \cdots q_r^{\beta_r},$$

where the exponents are non-negative integers, and we may suppose (after possibly swapping $\lambda$, $\mu$) that

(i) either $a = b = 0$ and $c > 0$,
(ii) or $b = c = 0$ and $a > 0$.

Let's look at (i). Then $u \equiv \pm 1 \pmod{4\ell}$ and $v \equiv \pm 1 \pmod{4\ell}$. Hence

$$w = u + v \equiv \pm 1 \pm 1 \pmod{4\ell}.$$

Therefore $w \equiv 2 \pmod{4\ell}$ or $0 \pmod{4\ell}$ or $-2 \pmod{4\ell}$. However, $\ell \nmid w$ since $\ell \neq q_i$ for $i = 1, \dots, r$. Hence $w \equiv \pm 2 \pmod{4\ell}$. Therefore $c = \mathrm{ord}_2(w) = 1$. Hence $\mathrm{ord}_2(\lambda) = a - c = -1$ and $\mathrm{ord}_2(\mu) = b - c = -1$. This establishes (7.2) for case (i). The proof of (7.2) in case (ii) is similar. □

From this Kara and Ozman deduce an analogue of Theorem 6.4 for complex quadratic fields.

**Theorem 7.6** (Kara and Ozman)**.** *Assume conjectures (I) and (II). Let* $\mathbb{N}^{\mathrm{sf}}$ *denote the set of squarefree natural numbers. Let* $\mathcal{F}$ *be the subset of* $d \in \mathbb{N}^{\mathrm{sf}}$ *for which the asymptotic Fermat conjecture holds over* $\mathbb{Q}(\sqrt{-d})$*. Then*

$$\liminf_{X \to \infty} \frac{\#\{d \in \mathcal{F} \ : \ d \le X\}}{\#\{d \in \mathbb{N}^{\mathrm{sf}} \ : \ d \le X\}} \ge 5/6.$$

**Remark.** It is interesting to compare Theorems 6.4 and 7.6. In the former, the asymptotic Fermat conjecture is established for almost all real quadratic fields, assuming the Eichler–Shimura conjecture. In the latter, even assuming the Eichler–Shimura conjecture and Serre's modularity conjecture, the asymptotic Fermat conjecture is established for 5/6 of imaginary quadratic fields. The reason for the disparity is that the conclusion of the Eichler–Shimura conjecture over real quadratic fields is stronger than that for the Eichler–Shimura conjecture over complex quadratic fields. Over a real quadratic field $K$ it is conjectured that a rational weight 2 Hilbert eigenform $\mathfrak{f}$ over $K$ corresponds to an elliptic curve $E/K$. Over a complex quadratic field $K$, it is conjectured that a rational weight 2 Bianchi eigenform over $K$ corresponds to either an elliptic curve $E/K$, or an abelian surface $A/K$ whose endomorphism algebra is an indefinite division quaternion algebra (such an abelian surface is called a **fake elliptic curve**). If 2 splits or ramifies in $K$ then the Frey curve has potentially multiplicative reduction at the primes above 2 and it is known that fake elliptic curves have potentially good reduction at all primes. An image of inertia argument then allows for the elimination of the fake elliptic curve case. Unfortunately if 2 is inert in $K$, then the Frey elliptic curve might

have potentially good reduction, and we are yet to find a way of eliminating the possiblity of a fake elliptic curve. We note that 2 is inert in $\mathbb{Q}(\sqrt{-d})$ if and only if $-d \equiv 5 \pmod 8$. This is 1/6 of all complex quadratic fields, and explains the numerical disparity between Theorems 6.4 and 7.6.

7.1. **Other Signatures.** An equation of the form $Ax^p + By^q = Cz^r$ is called the generalized Fermat equation of **signature** $(p, q, r)$. Thus (7.1) has signature $(p, p, p)$. Generalized Fermat equations of signatures $(p, p, 2)$ and $(p, p, 3)$ have good Frey curves and have been studied, with $K = \mathbb{Q}$, respectively by Bennett and Skinner [BS04] and by Bennett, Vatsal and Yazdani [BVY04]. More recently the techniques used by Freitas and Siksek and by Kara and Ozman have been applied by Isik, Kara and Ozman [IKO20] to study Fermat equations of signature $(p, p, 2)$ over number fields.

## References


[AKM+19] Alejandra Alvarado, Angelos Koutsianas, Beth Malmskog, Christopher Rasmussen, Christelle Vincent, and Mckenzie West, *A robust implementation for solving the S-unit equation and several applications*, arXiv e-prints (March 2019), arXiv:1903.00977, available at 1903.00977. ↑4

[BB17] Michael A. Bennett and Nicolas Billerey, *Sums of two S-units via Frey-Hellegouarch curves*, Math. Comp. **86** (2017), no. 305, 1375–1401. MR3614021 ↑4

[BGR19] Michael A. Bennett, Adela Gherga, and Andrew Rechnitzer, *Computing elliptic curves over* $\mathbb{Q}$, Math. Comp. **88** (2019), no. 317, 1341–1390. MR3904149 ↑5

[BMS16] Michael Bennett, Preda Mihăilescu, and Samir Siksek, *The generalized Fermat equation*, Open problems in mathematics, 2016, pp. 173–205. MR3526934 ↑2

[Bro06] Jerzy Browkin, *The abc-conjecture for algebraic numbers*, Acta Math. Sin. (Engl. Ser.) **22** (2006), no. 1, 211–222. MR2200778 ↑1, 7

[BS04] Michael A. Bennett and Chris M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54. MR2031121 ↑6, 7.1

[BVY04] Michael A. Bennett, Vinayak Vatsal, and Soroosh Yazdani, *Ternary Diophantine equations of signature* $(p, p, 3)$, Compos. Math. **140** (2004), no. 6, 1399–1416. MR2098394 ↑7.1

[Car83] Henri Carayol, *Sur les représentations l-adiques attachées aux formes modulaires de Hilbert*, C. R. Acad. Sci. Paris Sér. I Math. **296** (1983), no. 15, 629–632. MR705677 ↑2

[Coh07] Henri Cohen, *Number theory. Vol. II. Analytic and modern tools*, Graduate Texts in Mathematics, vol. 240, Springer, New York, 2007. MR2312338 ↑2

[ŞS18] Mehmet Haluk Şengün and Samir Siksek, *On the asymptotic Fermat's last theorem over number fields*, Comment. Math. Helv. **93** (2018), no. 2, 359–375. MR3811755 ↑2, 3, 6, 7

[Dec16] Heline Deconinck, *On the generalized Fermat equation over totally real fields*, Acta Arith. **173** (2016), no. 3, 225–237. MR3512853 ↑5, 5, 7

[Dic66] Leonard Eugene Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York, 1966. MR0245500 ↑1

[DK94] Olivier Debarre and Matthew J. Klassen, *Points of low degree on smooth plane curves*, J. Reine Angew. Math. **446** (1994), 81–87. MR1256148 ↑1

[DM97] Henri Darmon and Loïc Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. **490** (1997), 81–100. MR1468926 ↑2

[DS18] Luis Dieulefait and Eduardo Soto, *Solving* $ax^p + by^p = cz^p$ *with abc containing an arbitrary number of prime factors*, 2018. ↑7

[dW89] B. M. M. de Weger, *Algorithms for Diophantine equations*, CWI Tract, vol. 65, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989. MR1026936 ↑4, 5

[EG15] Jan-Hendrik Evertse and Kálmán Győry, *Unit equations in Diophantine number theory*, Cambridge Studies in Advanced Mathematics, vol. 146, Cambridge University Press, Cambridge, 2015. MR3524535 ↑4

[Eve84] Jan-Hendrik Evertse, *On equations in $S$-units and the Thue-Mahler equation*, Invent. Math. **75** (1984), no. 3, 561–584. MR735341 ↑4

[FKS20a] Nuno Freitas, Alain Kraus, and Samir Siksek, *Class field theory, Diophantine analysis and the asymptotic Fermat's Last Theorem*, Adv. Math. **363** (2020), 106964. MR4054049 ↑1, 6.1

[FKS20b] Nuno Freitas, Alain Kraus, and Samir Siksek, *On Asymptotic Fermat over $\mathbb{Z}_p$ extensions of $\mathbb{Q}$*, arXiv e-prints (March 2020), arXiv:2003.04029, available at 2003.04029. ↑6.1, 6.1

[FLHS15] Nuno Freitas, Bao V. Le Hung, and Samir Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), no. 1, 159–206. MR3359051 ↑3

[FS15a] Nuno Freitas and Samir Siksek, *The asymptotic Fermat's Last Theorem for five-sixths of real quadratic fields*, Compos. Math. **151** (2015), no. 8, 1395–1415. MR3383161 ↑6, 6

[FS15b] ———, *Criteria for irreducibility of* mod $p$ *representations of Frey curves*, J. Théor. Nombres Bordeaux **27** (2015), no. 1, 67–76. MR3346965 ↑3

[FS15c] ———, *Fermat's last theorem over some small real quadratic fields*, Algebra Number Theory **9** (2015), no. 4, 875–895. MR3352822 ↑1

[GR78] Benedict H. Gross and David E. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*, Invent. Math. **44** (1978), no. 3, 201–224. MR491708 ↑1

[Hid81] Haruzo Hida, *On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves*, Amer. J. Math. **103** (1981), no. 4, 727–776. MR623136 ↑3

[HK02] Emmanuel Halberstadt and Alain Kraus, *Courbes de Fermat: résultats et problèmes*, J. Reine Angew. Math. **548** (2002), 167–234. MR1915212 ↑7

[HP84] Fred H. Hao and Charles J. Parry, *The Fermat equation over quadratic fields*, J. Number Theory **19** (1984), no. 1, 115–130. MR751168 ↑1

[IKO20] Erman Isik, Yasemin Kara, and Ekin Ozman, *On ternary Diophantine equations of signature $(p, p, 2)$ over number fields*, preprint (2020). http://www.math.boun.edu.tr/postGraduate/yasemin.kara/Numberfield_newversion.pdf. ↑7.1

[JM04] Frazer Jarvis and Paul Meekin, *The Fermat equation over $\mathbb{Q}(\sqrt{2})$*, J. Number Theory **109** (2004), no. 1, 182–196. MR2098483 ↑1

[Kim05] Minhyong Kim, *The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel*, Invent. Math. **161** (2005), no. 3, 629–656. MR2181717 ↑4

[KM16] Rafael von Känel and Benjamin Matschke, *Solving $S$-unit, Mordell, Thue, Thue-Mahler and generalized Ramanujan-Nagell equations via Shimura-Taniyama conjecture*, 2016. ↑4

[KO20] Yasemin Kara and Ekin Ozman, *Asymptotic generalized Fermat's Last Theorem over number fields*, International Journal of Number Theory (2020), 1–18. ↑7

[Kol01] V. A. Kolyvagin, *On the first case of the Fermat theorem for cyclotomic fields*, 2001, pp. 3302–3311. Algebraic geometry, 11. MR1878050 ↑1

[Kra97] Alain Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. **49** (1997), no. 6, 1139–1161. MR1611640 ↑7

[Kra98] ———, *Sur l'équation $a^3 + b^3 = c^p$*, Experiment. Math. **7** (1998), no. 1, 1–13. MR1618290 ↑6

[LV18] Brian Lawrence and Akshay Venkatesh, *Diophantine problems and p-adic period mappings* (2018), available at 1807.02721. ↑4

[Rib97] Kenneth A. Ribet, *On the equation $a^p + 2^\alpha b^p + c^p = 0$*, Acta Arith. **79** (1997), no. 1, 7–16. MR1438112 ↑2

[Ser87] Jean-Pierre Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230. MR885783 ↑2

[Sik12] Samir Siksek, *The modular approach to Diophantine equations*, Explicit methods in number theory, 2012, pp. 151–179. MR3098134 ↑2

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, Second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 ↑5

[Sma98] Nigel P. Smart, *The algorithmic resolution of Diophantine equations*, London Mathematical Society Student Texts, vol. 41, Cambridge University Press, Cambridge, 1998. MR1689189 ↑4

[Sma99] ———, *Determining the small solutions to $S$-unit equations*, Math. Comp. **68** (1999), no. 228, 1687–1699. MR1653990 ↑4.7

[Ţur18] George C. Ţurcaş, *On Fermat's equation over some quadratic imaginary number fields*, Res. Number Theory **4** (2018), no. 2, Art. 24, 16. MR3798168 ↑1, 3

[Tri20a] Nicholas Triantafillou, *Restriction of scalars Chabauty and the S-unit equation* (2020), available at `2006.10590`. ↑4

[Tri20b] Nicholas Triantafillou, *The unit equation has no solutions in number fields of degree prime to* 3 *where* 3 *splits completely*, arXiv e-prints (March 2020), arXiv:2003.02414, available at `2003.02414`. ↑4

[TW95] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572. MR1333036 ↑1

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR1333035 ↑1

Bogazici University, Department of Mathematics, Bebek, Istanbul, 34342, Turkey
*Email address*: `ekin.ozman@boun.edu.tr`

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