INTEGERS THAT ARE SUMS OF TWO CUBES IN THE CYCLOTOMIC $\mathbb{Z}_p$-EXTENSION

ANWESH RAY

ABSTRACT. Let n be a cubefree natural number and $p \geq 5$ be a prime number. Assume that n is not expressible as a sum of the form $x^3 + y^3$, where $x, y \in \mathbb{Q}$. In this note, we study the solutions (or lack thereof) to the equation $n = x^3 + y^3$, where x and y belong to the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. As an application, consider the case when n is not a sum of rational cubes. Then, we prove that n cannot be a sum of two cubes in certain large families of prime cyclic extensions of $\mathbb{Q}$.

1. INTRODUCTION

Given a natural number n, and $k \in \mathbb{Z}_{\geq 2}$, it is of natural interest to investigate if n may be represented as a sum of two k-th powers

$$n = x^k + y^k,$$

where x and y are rational numbers. The problem has been completely solved by Euler when $k = 2$, and in this case, it is easy to see that n is a sum of two rational squares if and only if it is a sum of two integers squares. It turns out that n is a sum of two integer squares if all prime factors ℓ of n such that $\ell \equiv 1 \mod 4$ have even exponent in the factorization of n. It follows from this description that the natural density of numbers that can be represented as a sum of two rational squares is 0. On the other hand, it is possible for n to be a sum of two rational cubes without being a sum of two integer cubes. The smallest example is

$$6 = \left(\frac{17}{21}\right)^3 + \left(\frac{37}{21}\right)^3.$$

It is expected that the density of natural numbers n that can be represented as a sum of two rational cubes is $\frac{1}{2}$, cf. [ABS22]. There has been much work done on the problem of determining when n is a sum of rational cubes and the problem goes back to work of Sylvester [Syl80], Selmer [Sel51], Satgé [Sat87] and Lieman [Lie94]. More recently, Alpöge, Bhargava and Schnidman [ABS22] showed that the lower density of natural numbers n that are (resp. are not) a sum of two rational cubes is $\geq \frac{2}{21}$ (resp $\geq \frac{1}{6}$).

In this article we consider a related question. Suppose n is *not* expressible as a sum of two rational cubes and L is an algebraic extension of $\mathbb{Q}$. We seek conditions for n to not equal $x^3 + y^3$, for all $x, y \in L$. The extensions L we shall consider are infinite cyclotomic extensions that have come to prominence thanks to celebrated work of Iwasawa, cf.

[Iwa73] and [Was97, Ch. 13]. Fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. Let $p \geq 5$ be a prime number and $\mathbb{Q}(\mu_{p^\infty}) \subset \bar{\mathbb{Q}}$ be the infinite cyclotomic extension of $\mathbb{Q}$ generated by all p-power roots of unity. Via the cyclotomic character, the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_p^\times$, the units in $\mathbb{Z}_p$. This group decomposes into a product $\Delta \times U$, where $\Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and $U = 1 + p\mathbb{Z}_p$ is the subgroup of principal units in $\mathbb{Z}_p^\times$. The p-adic logarithm gives an isomorphism of U with the additive group $\mathbb{Z}_p$. Let $\mathbb{Q}_\infty^{(p)}$ be the subfield of $\mathbb{Q}(\mu_{p^\infty})$ that is fixed by Δ. By construction, $\mathbb{Q}_\infty^{(p)}$ is a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}_p$. This extension is referred to as the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Being a pro-p abelian extension of $\mathbb{Q}$, the cyclotomic $\mathbb{Z}_p$-extension satisfies some nice properties. All primes are finitely decomposed in $\mathbb{Q}_\infty^{(p)}$ and the only prime that ramifies is p. It is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Let E_n denote the elliptic curve defined by $x^3 + y^3 = nz^3$. This elliptic curve is seen to have no nontrivial rational torsion points. Therefore n is a sum of two rational cubes if and only if the rank of $E_n(\mathbb{Q})$ is positive. The growth of ranks of elliptic curves in $\mathbb{Z}_p$-extensions of number fields was studied by Mazur, cf. [Maz72]. Kato [K+04] and Rohrlich [Roh84] proved that given an elliptic curve $E_{/\mathbb{Q}}$, the rank of $E(\mathbb{Q}_n^{(p)})$ is bounded as n goes to ∞. Moreover the upper bound can be related to the algebraic structure of Selmer groups defined over $\mathbb{Q}_\infty^{(p)}$. The conjectural properties of these Selmer groups were described by Mazur, and later Rubin [Rub81] and Kato [K+04] showed that they are cotorsion as modules over the Iwasawa algebra. The structure of such groups are closely related to analytic objects known as p-adic L-functions.

In this article, we employ techniques from the Iwasawa theory of Selmer groups to study the following question.

Question 1.1. *Let n be a cubefree natural number which is not the sum of two rational cubes. Let $p \geq 5$ be a prime at which the elliptic curve*

$$E_n : x^3 + y^3 = nz^3$$

has good ordinary reduction. Then, can n be a sum of the form $x^3 + y^3$, where $x, y \in \mathbb{Q}_\infty^{(p)}$.

Theorem 1.2. *Let n be a cubefree natural number which is not the sum of two cubes in $\mathbb{Q}$. Assume that the Tate-Shafarevich group $\mathrm{III}(E_n/\mathbb{Q})$ is finite. Let S be the set of prime numbers $p \geq 5$ such that*

    (a) E_n has good ordinary reduction at p,
    (b) $\mathrm{III}(E_n/\mathbb{Q})[p] = 0$,
    (c) p does not divide $|\widetilde{E}_n(\mathbb{F}_p)|$, where $\widetilde{E}_n$ is the reduction of E_n modulo p.

Then the following assertions hold

    (1) S has density $\frac{1}{2}$.
    (2) For any prime $p \in S$, n is not a sum of two cubes in $\mathbb{Q}_\infty^{(p)}$.

The assumption that $p \geq 5$ in Theorem 1.2 is necessary since it is assumed that E_n has good reduction at p. On the other hand, the curves E_n have bad reduction at $2, 3$. Our methods rely on the aforementioned results of Rubin and Kato, which is only valid for elliptic curves with good ordinary reduction at p. Since the elliptic curves in question

have complex multiplication, the density of primes of good ordinary (resp. supersingular) reduction is $\frac{1}{2}$ (resp. $\frac{1}{2}$). In effect, we show that the set of primes for which our result holds is of density 1 in the set of primes of good ordinary reduction. On the other hand, if p is a prime of good ordinary reduction such that $\mathrm{Sel}_{p^\infty}(E_n/\mathbb{Q}_\infty^{(p)}) \neq 0$, then this does not necessarily mean that $E_n(\mathbb{Q}_\infty^{(p)}) \neq 0$, since the contribution could as well arise from growth in the p-primary part of the Tate-Shafarevich group. Using Theorem 1.2 we obtain the following unexpected result on the non-solvability of the equation $n = x^3 + y^3$ in certain prime cyclic extensions of $\mathbb{Q}$.

Theorem 1.3. *Let n be a cube-free natural number which is not a sum of cubes in $\mathbb{Q}$ and let $p > 7$ be a prime number in the set S described in Theorem 1.2. Let $L/\mathbb{Q}$ be a Galois extension with Galois group $G := \mathrm{Gal}(L/\mathbb{Q})$ and let Σ be the primes ℓ that ramify in L. Assume that*

(1) $G \simeq \mathbb{Z}/p\mathbb{Z}$,
(2) the primes $\ell \in \Sigma$ do not divide $6pn$,
(3) for primes $\ell \in \Sigma$, we assume that $\widetilde{E}_n(\mathbb{F}_\ell)[p] = 0$.

Then, n cannot be represented as $x^3 + y^3$ for $x, y \in L$.

In fact, our method shows that n cannot be a sum of two cubes in the cyclotomic $\mathbb{Z}_p$-extension of L. This result is proven by showing that the Iwasawa μ- and λ-invariants are trivial for the Selmer group considered over this $\mathbb{Z}_p$-extension. The key ingredient is an analogue of *Kida's formula*, due to Hachimori and Matsuno [HM99], which studies the growth of such Iwasawa invariants in p-extensions. Given an elliptic curve $E_{/\mathbb{Q}}$ with $\mathrm{End}_{\bar{\mathbb{Q}}}(E) = \mathrm{End}_\mathbb{Q}(E)$, it follows from the results of Mazur and Rubin [MR18] on *diophantine stability* that for a positive density of primes, there will exist infinitely many $L/\mathbb{Q}$ for which $E(L) = E(\mathbb{Q})$. For elliptic curves E_n, our result applies to all prime numbers $p > 7$ that lie in the explicitly defined set S.

1.1. **Outlook and related work.** In recent years, there has been growing momentum in the study of solutions to diophantine equations in cyclotomic towers of number fields, bridging seemingly disparate themes in number theory. For instance, Freitas, Kraus and Siksek [FKS20a, FKS20b] studied the Fermat equation $x^\ell + y^\ell = z^\ell$ in cyclotomic towers over $\mathbb{Q}$. The author and Weston merged diophantine methods with Galois cohomological ideas from Iwasawa theory [RW24] to prove special cases of Hilbert's tenth problem in anticyclotomic towers of imaginary quadratic fields.

1.2. **Organization.** Including the introduction the article consists of three sections. In the second section, we introduce notation and preliminaries on the Iwasawa theory of elliptic curves. In the final section, we prove the Theorems 1.2 and 1.3. We finish with an explicit example to illustrate these results.

Acknowledgement. The author wishes to thank the referee for the helpful report.

2. IWASAWA THEORY OF ELLIPTIC CURVES

Let n be a cube-free natural number and let E_n be the elliptic curve defined by the Weierstrass equation

$$E_n : x^3 + y^3 = nz^3.$$

It is well known that $E_n(\mathbb{Q})_{\text{tors}} = 0$ and thus, n can be represented by a sum of two rational cubes if and only if $\text{rank}\, E_n(\mathbb{Q}) > 0$. The Weierstrass form of the curve E_n is given by $y^2 = x^3 - 432n^2$. It is easy to see that E_n has good reduction at all primes $p \nmid 6n$. For the rest of this section, E is an elliptic curve defined over $\mathbb{Q}$. A finite Galois extension $L/\mathbb{Q}$ is said to be a p-extension if $\# \text{Gal}(L/\mathbb{Q})$ is a power of p. A Galois extension $L/\mathbb{Q}$ which is an increasing union of p-extensions is referred to as a pro-p extension of $\mathbb{Q}$. For a natural number m, let $E[m]$ denote the m-torsion subgroup of $E(\bar{\mathbb{Q}})$ and

$$\rho_{E,m} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

the associated Galois representation. The field $\mathbb{Q}(E[m])$ is the fixed field of the kernel of $\rho_{E,m}$. We note that $\mathbb{Q}(E[m])$ is a Galois extension of $\mathbb{Q}$ whose Galois group can be identified with the image of $\rho_{E,m}$. Given a number field F, we set $F(E[m])$ to denote the composite of F with $\mathbb{Q}(E[m])$.

Lemma 2.1. *Let n be a cube-free natural number and L be a pro-p extension of $\mathbb{Q}$. Assume that $p \nmid 6n$ and that p is totally ramified in L. Then, n is a sum of two cubes $x, y \in L$ if and only if $\text{rank}\, E_n(L) > 0$.*

Proof. Let $E := E_n$, we show that $E(L)_{\text{tors}} = 0$. Since L is a union of finite p-extensions, we may assume without loss of generality that $L/\mathbb{Q}$ is a finite p-extension. It suffices to show that for all prime numbers q, we have that $E(L)[q] = 0$. First consider the case when $q = p$. Since $L/\mathbb{Q}$ is a p-extension, it follows from [NSW08, Proposition 1.6.12] that

$$E(\mathbb{Q})[p] = 0 \Rightarrow E(L)[p] = 0.$$

Next, we consider the case when $q \neq p$, then, the prime p is unramified in $\mathbb{Q}(E[q])$. On the other hand, since p is totally ramified in L, it follows that $L \cap \mathbb{Q}(E[q]) = \mathbb{Q}$. As a consequence, we find that $\text{Gal}(L(E[q])/L) \simeq \text{Gal}(\mathbb{Q}(E[q])/\mathbb{Q})$, and therefore,

$$E(\mathbb{Q})[q] = 0 \Rightarrow E(L)[q] = 0.$$

$\square$

Let p be an odd prime number and $\mathbb{Z}_p$ denote the ring of p-adic integers. The *cyclotomic $\mathbb{Z}_p$-extension* $\mathbb{Q}_\infty^{(p)}/\mathbb{Q}$ is the unique $\mathbb{Z}_p$-extension contained in $\mathbb{Q}(\mu_{p^\infty})$. Let $\mathbb{Q}_n^{(p)}$ be the extension of $\mathbb{Q}$ that is contained in $\mathbb{Q}_\infty^{(p)}$ such that $[\mathbb{Q}_n^{(p)} : \mathbb{Q}] = p^n$. We refer to $\mathbb{Q}_n^{(p)}$ as the *n-th layer*. Let K be a field of characteristic 0 and E be an elliptic curve over $\mathbb{Q}$. We set $\bar{K}$ to be a choice of algebraic closure of K and G_K denote the Galois group $\text{Gal}(\bar{K}/K)$. When it is clear from the context, set $E := E(\bar{K})$ and $E[p^n] := E(\bar{K})[p^n]$. Consider the exact sequence of G_K-modules

$$0 \to E[p^n] \to E \xrightarrow{\times p^n} E \to 0,$$

associated to which is the exact sequence

$$0 \to E(K) \otimes \left(\mathbb{Z}/p^n\mathbb{Z}\right) \to H^1(\text{G}_K, E[p^n]) \to H^1(\text{G}_K, E)[p^n] \to 0.$$

Taking direct limits as $n \to \infty$, obtain a short exact sequence

$$0 \to E(K) \otimes \left(\mathbb{Q}_p/\mathbb{Z}_p\right) \to H^1(\text{G}_K, E[p^\infty]) \to H^1(\text{G}_K, E)[p^\infty] \to 0.$$

Let F be a number field. For each non-archimedian prime v of F, let F_v denote the completion of F at v. Choose an embedding $\iota_v : \bar{F} \hookrightarrow \bar{F}_v$ for each prime v, and

$$\iota_v^* : \mathrm{G}_{F_v} \hookrightarrow \mathrm{G}_F$$

the associated embedding. This embedding induces the restriction map

$$\mathrm{res}_v : H^1(\mathrm{G}_F, E[p^\infty]) \to H^1(\mathrm{G}_{F_v}, E[p^\infty]).$$

The p-primary Selmer group over F is defined as follows

$$\mathrm{Sel}_{p^\infty}(E/F) := \left\{ c \in H^1(\mathrm{G}_\mathbb{Q}, E[p^\infty]) \mid \mathrm{res}_v(c) \in E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \text{ for all primes } v \right\}.$$

For a number field F, denote by $\mathrm{III}(E/F)$ the *Tate-Shafarevich group*

$$\mathrm{III}(E/F) := \left\{ H^1(\bar{F}/F, E) \to \prod_v H^1(\bar{F}_v/F_v, E) \right\}.$$

The Selmer group is an extension of the Tate-Shafarevich group, there is a short exact sequence

(2.1) $$0 \to E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/F) \to \mathrm{III}(E/F)[p^\infty] \to 0.$$

When $F/\mathbb{Q}$ is Galois, the Selmer group is a module over $\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]$. The Selmer group over $\mathbb{Q}_\infty^{(p)}$ is defined to be the following direct limit

$$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty^{(p)}) := \varinjlim_{n \to \infty} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n^{(p)}).$$

Let Γ denote the Galois group $\mathrm{Gal}(\mathbb{Q}_\infty^{(p)}/\mathbb{Q})$ and let γ be a topological generator of Γ. The Iwasawa algebra Λ is the completed group algebra

$$\Lambda := \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma^{p^n}].$$

Set $T := \gamma - 1$ and identify Λ with the formal power series ring $\mathbb{Z}_p[\![T]\!]$. The dual Selmer group

$$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty^{(p)})^\vee := \mathrm{Hom}_{\mathrm{cnts}}\left(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty^{(p)}), \mathbb{Q}_p/\mathbb{Z}_p\right)$$

is the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty^{(p)})$. It follows from results of Kato [K$^+$04] that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty^{(p)})^\vee$ is finitely generated and torsion as a module over Λ.

Set M to denote the dual Selmer group of E over $\mathbb{Q}_\infty^{(p)}$. A polynomial $f(T) \in \mathbb{Z}_p[T]$ is *distinguished* if it is a monic polynomial whose nonleading coefficients are divisible by p. By the structure theory of finitely generated and torsion modules over Λ, there is a homomorphism

$$M \longrightarrow \left(\bigoplus_{i=1}^s \frac{\Lambda}{(p^{\mu_i})} \right) \oplus \left(\bigoplus_{i=1}^t \frac{\Lambda}{(f_j(T))} \right),$$

whose kernel and cokernel are both finite (see [Was97, Chapter 13]). In the above decomposition, $f_j(T)$ is a distinguished polynomial. The *characteristic element* is defined as follows

$$f_M(T) := \prod_i p^{\mu_i} \times \prod_j f_j(T).$$

This element decomposes into a product

$$f_M(T) = p^\mu \times g(T),$$

where $\mu \in \mathbb{Z}_{\geq 0}$ and $g(T)$ is a distinguished polynomial. The μ-invariant is the quantity $\mu = \sum_i \mu_i$ in the above decomposition. The λ-invariant is the degree of $g(T)$. The μ and λ-invariants of $\operatorname{Sel}_{p^\infty}(E/\mathbb{Q}_\infty^{(p)})^\vee$ over $\mathbb{Q}_\infty^{(p)}$ are denoted $\mu_p(E)$ and $\lambda_p(E)$ respectively. Denote by j_E the j-invariant of E.

Theorem 2.2. *Let $p \geq 5$ be a prime number at which E has good ordinary reduction such that*

    (1) p does not divide $|\widetilde{E}(\mathbb{F}_p)|$, where $\widetilde{E}$ is the reduction of E modulo p,
    (2) if E has split multiplicative reduction at $\ell \neq p$, then, $p \nmid \operatorname{ord}_\ell(j_E)$.

Then there is a natural map

$$\operatorname{Sel}_{p^\infty}(E/\mathbb{Q}) \to \operatorname{Sel}_{p^\infty}(E/\mathbb{Q}_\infty^{(p)})^\Gamma$$

which is surjective. In particular, if $\operatorname{Sel}_{p^\infty}(E/\mathbb{Q}) = 0$, then, $\operatorname{Sel}_{p^\infty}(E/\mathbb{Q}_\infty^{(p)}) = 0$.

Proof. The above result is due to Greenberg, cf [Gre99a, Proposition 3.8]. $\qquad\square$

Let Π be the set of all primes $p \geq 5$ at which E has good ordinary reduction. For a subset $S \subset \Pi$ and let $S(x) := \{p \in S \mid p \leq x\}$. The natural density of S is the limit

$$\mathfrak{d}(S) := \lim_{x \to \infty} \frac{\#S(x)}{\#\Pi(x)}.$$

Corollary 2.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})$ and $\operatorname{III}(E/\mathbb{Q})$ are finite. Let S_E be the set of primes $p \geq 5$ at which E has good ordinary reduction and $\operatorname{Sel}_{p^\infty}(E/\mathbb{Q}_\infty^{(p)}) = 0$. Then, we find that $\mathfrak{d}(S_E) = 1$.*

Proof. It is known that $p \nmid |\widetilde{E}(\mathbb{F}_p)|$ for a density 1 set of primes p, cf. [Mur97]. The result then follows from Theorem 2.2. $\qquad\square$

3. Proof of the main results

In this section, we prove our main result. Throughout this section, n is a cube-free natural natural number and let E_n be the elliptic curve defined by the Weierstrass equation

$$E_n : x^3 + y^3 = nz^3.$$

Lemma 3.1. *Let $p \nmid 6n$ be an odd prime number at which E_n has good ordinary reduction and $\mathbb{Q}_\infty^{(p)}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. The following conditions are equivalent*

    (1) n is not a sum of two cubes in $\mathbb{Q}_\infty^{(p)}$.
    (2) $\operatorname{rank} E_n(\mathbb{Q}_\infty^{(p)}) = 0$.

Proof. The result follows from Lemma 2.1. $\qquad\square$

Proof of Theorem 1.2. The elliptic curve $E := E_n$ is a cubic twist of E_1 and thus has complex multiplication, and in this setting, the set of primes p at which E has good ordinary reduction has density $\frac{1}{2}$. By assumption, n is not a sum of two rational cubes, hence, $E(\mathbb{Q}) = 0$. After a change of coordinates, E_n is given by the equation $y^2 =$

$x^3 - 432n^2$. Thus in particular, there are no primes at which E has multiplicative reduction. Let $p \in S$, then, since $E(\mathbb{Q}) = 0$ and $\text{III}(E/\mathbb{Q})[p] = 0$, it follows from (2.1) that $\text{Sel}_{p^\infty}(E/\mathbb{Q}) = 0$. Theorem 2.2 then implies that $\text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty^{(p)}) = 0$ for all primes $p \in S$. The short exact sequence

$$0 \to E(\mathbb{Q}_\infty^{(p)}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty^{(p)}) \to \text{III}(E/\mathbb{Q}_\infty^{(p)})[p^\infty] \to 0$$

implies that $E(\mathbb{Q}_\infty^{(p)}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$. This gives that the rank of $E(\mathbb{Q}_\infty^{(p)})$ is 0. It then follows from Lemma 3.1 that for all $p \in S$, $E(\mathbb{Q}_\infty^{(p)}) = 0$, i.e., n cannot be represented as $x^3 + y^3$ for $x, y \in \mathbb{Q}_\infty^{(p)}$. The density of primes p at which $\widetilde{E}(\mathbb{F}_p)[p] \neq 0$ is 0 (cf. [Mur97]). This is indeed weaker than what is predicted by the Lang-Trotter conjecture, a precise unconditional asymptotic is obtained in *loc. cit.* It follows that the density of S is equal to the density of primes p at which E has good ordinary reduction. Therefore, the density of S is equal to $\frac{1}{2}$. $\qquad\square$

Proof of Theorem 1.3. Setting $E := E_n$, it suffices to show that $\text{rank}\, E(L) = 0$ and $E(L)_{\text{tors}} = 0$. Let $L_\infty^{(p)} := L \cdot \mathbb{Q}_\infty^{(p)}$, i.e., the cyclotomic $\mathbb{Z}_p$-extension of L. We recall from the proof of Theorem 1.2 that $\text{Sel}(E/\mathbb{Q}_\infty^{(p)}) = 0$. In particular, the μ- and λ-invariants of $\text{Sel}(E/\mathbb{Q}_\infty^{(p)})$ are equal to 0. It follows from our assumptions on p and n and the main result of [HM99] that the μ- and λ-invariants of $\text{Sel}(E/L_\infty^{(p)})$ are both equal to 0 (see [Ray23, Lemma 4.10] and its proof for further details). This implies in particular that the rank of $E(L)$ is 0 (cf. [Gre99b, Theorem 1.9]).

Since n is not expressible as a sum of rational cubes, we have that $E(\mathbb{Q}) = 0$, and in particular, $E(\mathbb{Q})_{\text{tors}} = 0$. It follows from [GJN20, Theorem 7.2] that since $p > 7$, $E(L)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}} = 0$. Therefore, $E(L) = 0$ and hence, n cannot be represented as $x^3 + y^3$ for any $x, y \in L$. $\qquad\square$

An example. Let us consider an explicit example. The number $n = 3$ is not a sum of two rational cubes. This can be seen by considering the elliptic curve $E := E_3 : x^3 + y^3 = 3$. In standard form, the equation of this curve is $E : y^2 = x^3 - 3888$. The data provided to us on LMFDB (see 243b2) confirms that this elliptic curve has trivial Mordell–Weil group over $\mathbb{Q}$. This elliptic curve has good ordinary reduction at 7, and $\#\widetilde{E}(\mathbb{F}_7) = 3$. In particular, 7 does not divide $\#\widetilde{E}(\mathbb{F}_7) = 3$. Moreover, the exact order of the Tate–Shafarevich group is 1. Thus, we find that 7 is contained in the set S defined in Theorem 1.2. The Theorem thus asserts that 3 is not a sum of cubes in the cyclotomic $\mathbb{Z}_7$-extension of $\mathbb{Q}$. Now let $L/\mathbb{Q}$ be the unique $\mathbb{Z}/7\mathbb{Z}$-extension of $\mathbb{Q}$ which is contained in $\mathbb{Q}(\mu_{29})$. The set of primes Σ introduced in Theorem 1.3 is the single prime $\{29\}$. We find that

$$\#\widetilde{E}(\mathbb{F}_{29}) = 29 + 1 - a_{29}(E) = 30.$$

Therefore, we have that $\widetilde{E}(\mathbb{F}_{29})[7] = 0$. Thus, the conditions of Theorem 1.3 are satisfied, and we conclude that 3 is not representable as $x^3 + y^3$ for $x, y \in L$.

REFERENCES

[ABS22] Levent Alpöge, Manjul Bhargava, and Ari Shnidman. Integers expressible as the sum of two rational cubes. *arXiv preprint arXiv:2210.10730*, 2022.

[FKS20a] Nuno Freitas, Alain Kraus, and Samir Siksek. Class field theory, Diophantine analysis and the asymptotic Fermat's last theorem. *Adv. Math.*, 363:106964, 37, 2020.

[FKS20b] Nuno Freitas, Alain Kraus, and Samir Siksek. On asymptotic Fermat over $\mathbb{Z}_p$-extensions of
          $\mathbb{Q}$. *Algebra Number Theory*, 14(9):2571–2574, 2020.
[GJN20]   Enrique González-Jiménez and Filip Najman. Growth of torsion groups of elliptic curves upon
          base change. *Math. Comp.*, 89(323):1457–1485, 2020.
[Gre99a] Ralph Greenberg. Iwasawa theory for elliptic curves. In *Arithmetic theory of elliptic curves
          (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Math.*, pages 51–144. Springer, Berlin, 1999.
[Gre99b] Ralph Greenberg. Iwasawa theory for elliptic curves. In *Arithmetic theory of elliptic curves
          (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Math.*, pages 51–144. Springer, Berlin, 1999.
[HM99]   Yoshitaka Hachimori and Kazuo Matsuno. An analogue of Kida's formula for the Selmer groups
          of elliptic curves. *J. Algebraic Geom.*, 8(3):581–601, 1999.
[Iwa73]   Kenkichi Iwasawa. On $\mathbb{Z}_\ell$-extensions of algebraic number fields. *Ann. of Math. (2)*, 98:246–326,
          1973.
[K$^+$04] Kazuya Kato et al. p-adic Hodge theory and values of zeta functions of modular forms.
          Astérisque, 295:117–290, 2004.
[Lie94]   Daniel B. Lieman. Nonvanishing of L-series associated to cubic twists of elliptic curves. *Ann.
          of Math. (2)*, 140(1):81–108, 1994.
[Maz72]   Barry Mazur. Rational points of abelian varieties with values in towers of number fields.
          Inventiones mathematicae, 18(3-4):183–266, 1972.
[MR18]   Barry Mazur and Karl Rubin. Diophantine stability. *Amer. J. Math.*, 140(3):571–616, 2018.
          With an appendix by Michael Larsen.
[Mur97]   V. Kumar Murty. Modular forms and the Chebotarev density theorem. II. In *Analytic number
          theory (Kyoto, 1996)*, volume 247 of *London Math. Soc. Lecture Note Ser.*, pages 287–308.
          Cambridge Univ. Press, Cambridge, 1997.
[NSW08]   Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, vol-
          ume 323 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of
          Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.
[Ray23]   Anwesh Ray. Arithmetic statistics and diophantine stability for elliptic curves. *Ramanujan J.*,
          62(1):215–239, 2023.
[Roh84]   David E. Rohrlich. On L-functions of elliptic curves and cyclotomic towers. *Invent. Math.*,
          75(3):409–423, 1984.
[Rub81]   Karl Rubin. Elliptic curves with complex multiplication and the conjecture of Birch and
          Swinnerton-Dyer. *Invent. Math.*, 64(3):455–470, 1981.
[RW24]   Anwesh Ray and Tom Weston. Hilbert's tenth problem in anticyclotomic towers of number
          fields. *Trans. Amer. Math. Soc.*, 377(5):3577–3597, 2024.
[Sat87]   Philippe Satgé. Un analogue du calcul de Heegner. *Invent. Math.*, 87(2):425–439, 1987.
[Sel51]   Ernst S. Selmer. The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 85:203–362 (1
          plate), 1951.
[Syl80]   J. J. Sylvester. On Certain Ternary Cubic-Form Equations. *Amer. J. Math.*, 3(1):58–88, 1880.
[Was97]   Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science &
          Business Media, 1997.

(Ray) Chennai Mathematical Institute, H1, SIPCOT IT Park, Kelambakkam, Siruseri,
Tamil Nadu 603103, India

Email address: anwesh@cmi.ac.in