Binary cubic forms and rational cube sum problem

Somnath Jha[1], Dipramit Majumdar[2*†], B. Sury[3†]

[1]Department of of Mathematics & Statistics, Indian Institute of Technology Kanpur, Kalyanpur, Kanpur, 208016, Uttar Pradesh, India.
[2*]Department of Mathematics, Indian Institute of Technology Madras, Chennai, 600036, Tamilnadu, India.
[3]Stat-Math Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore, 560059, Karnataka, India.

*Corresponding author(s). E-mail(s): dipramit@gmail.com;
Contributing authors: jhasom@gmail.com; surybang@gmail.com;
†These authors contributed equally to this work.

Abstract

The classical Diophantine problem of determining which integers can be written as a sum of two rational cubes has a long history; from the earlier works of Sylvester, Selmer, Satgé, Lieman etc. and up to the recent work of Alpöge-Bhargava-Shnidman. In this note, we use binary cubic forms to study the rational cube sum problem. We prove (unconditionally) that for any positive integer $\boldsymbol{d}$, infinitely many primes in each of the residue classes $\mathbf{1 \pmod{9d}}$ as well as $\mathbf{-1 \pmod{9d}}$, are sums of two rational cubes. Among other results, we prove that every non-zero residue class $\boldsymbol{a} \pmod{\boldsymbol{q}}$, for any prime $\boldsymbol{q}$, contains infinitely many primes which are sums of two rational cubes. Further, for an arbitrary integer $\boldsymbol{N}$, we show there are infinitely many primes $\boldsymbol{p}$ in each of the residue classes $\mathbf{8 \pmod 9}$ and $\mathbf{1 \pmod 9}$, such that $\boldsymbol{Np}$ is a sum of two rational cubes.

Keywords: Binary cubic forms, primes represented by binary cubic forms, rational cube sum problem, $\mathbf{\pm 1 \pmod 9}$ cases of Sylvester's conjecture

MSC Classification: Primary 11D25 , 11N32; Secondary 11N13 , 11G05

1 Introduction

Let us call an integer n a rational cube sum if there exist two rational numbers a and b such that $n = a^3 + b^3$. The study of which integers n are rational cube sums has a rich history and can be traced back to the classical works of Sylvester [1], Selmer [2], Satgé [3], Lieman [4] and up to a very recent work of Alpöge-Bhargava-Shnidman [5]. Without any loss of generality, we may assume that n is cube free and greater than 2. Then the elliptic curve $Y^3 + X^3 = nZ^3$, expressed in Weierstrass form as $E_n : Y^2 = X^3 - 432n^2$, has $E_n(\mathbb{Q})_{\text{tor}} = 0$ and it is easy to see that n is a rational cube sum $\Leftrightarrow \text{rank}_{\mathbb{Z}}\ E_n(\mathbb{Q}) > 0$. The important work of [5] shows that, when ordered by their absolute value, a positive proportion of integers are rational cube sums and a positive proportion are not.

In a special case of prime numbers, there is a conjecture, typically attributed to Sylvester (see [6]), on the expressibility of primes as rational cube sums. This predicts that primes $p \equiv 2, 5 \pmod 9$ are not rational cube sums, whereas primes $p \equiv 4, 7, 8 \pmod 9$ are rational cube sums. In contrast, primes $p \equiv 1 \pmod 9$ may or may not be rational cube sums. The proof of the fact that primes $p \equiv 2, 5 \pmod 9$ are not cube sums goes back to the works of Pépin, Lucas and Sylvester [1]. Dasgupta-Voight [6], showed that for primes $p \equiv 4, 7 \pmod 9$, both p and p^2 are rational cube sums provided 3 is not a cube modulo p.

The questions on the expressibility of primes $p \equiv 8 \pmod 9$ are reported to be 'decidedly more difficult' (see [6], [7]). It seems the only general known result so far is due to [7], which shows for a prime $p \equiv 8 \pmod 9$, if $x^9 - 24x^6 + 3x^3 + 1 - 9(\sqrt[3]{3} - 1)x^2(x^3 + 1)^2 = 0$ has no solutions in $\mathbb{F}_p$, then at least one of p and p^2 is a rational cube sum. The works of [6] and [7], although different, use the theory of (mock) Heegner points. To determine which primes $p \equiv 1 \pmod 9$ are rational cube sums seems to be a rather subtle question and was investigated in [8]. The Birch and Swinnerton-Dyer conjecture predicts that the special value of the complex L-function of E_p at 1 i.e. $L(E_p/\mathbb{Q}, 1) = *C_p$, where $* \neq 0$ and $C_p = 0$ if and only if p is a rational cube sum. In [8], three efficient methods are given to numerically test whether $C_p = 0$ for a prime $p \equiv 1 \pmod 9$.

In fact, cube sum problem in congruence classes (modulo a prime) has also been studied using analytic methods. In an interesting work, Lieman using the analytic properties of L-function of CM elliptic curves together with Coates-Wiles theorem, showed the following:

Theorem 1.1. *[4, Theorem 0.1] Fix a prime $q > 3$, and a congruence class $a \pmod q$. There exist infinitely many cube-free n congruent to $a \pmod q$ such that n can not be expressed as a sum of two rational cubes.*

On a different note, a celebrated work of Heath-Brown [9], using Sieve theoretic methods, showed that the integer values of the binary cubic form X^3+2Y^3 represents infinitely many primes. This was generalised by Heath-Brown and Moroz, to a general irreducible integral binary cubic form in [10], and then in [11], in a way which is more amenable to control congruence classes represented by the primes.

In this note, we use some special integral binary cubic forms (like $(X+Y)^3 - 9XY^2$, $XY(X - Y)$, $N(X^3+NY^3)$) whose integer values are rational cube sums. Then we exploit various polynomial identities satisfied by these special polynomials and use infinitude of primes represented by suitable binary cubic forms in congruence classes [11] to obtain various infinite families of rational cube sum integers. Evidently, this approach is different from the recent works based on Selmer groups of elliptic curves and Heegner points.

In fact, in a previous article [12] by two of us, using the explicit parametrization of integral points on the curve $X^2 + 27Y^2 = 4Z^3$ together with the result in [10], it was shown that there are infinitely many primes p, congruent to either $1 \pmod 9$ or $8 \pmod 9$, such that p is a sum of two rational cubes. Subsequently, Prof. Moroz and also Prof. Heath-Brown wrote to us pointing out that using [11], we can significantly improve our previous result. We prove:

Theorem A (Theorem 2.4 & Corollary 2.11)**.** *For any positive integer d and any integer $a \equiv \pm 1 \pmod 9$ satisfying $(a, d) = 1$, there are infinitely many primes $p \equiv a \pmod{9d}$ which are rational cube sums.*

In particular, infinitely many primes in each of the residue classes $1 \pmod 9$ and $8 \pmod 9$ are rational cube sums. Each of these primes is a value of the cubic form $(X + Y)^3 - 9XY^2$ at certain integer point, which depends on the congruence class. □

Remark 1.2. *According to [6],[7], [8] and others, the cube sum problem for primes congruent to $8 \pmod 9$ and $1 \pmod 9$, is considered to be a difficult and subtle problem. Theorem 2.4 is the first unconditional result showing existence of infinitely many primes in each of these classes which are rational cube sums.*

Remark 1.3. *In [8], the authors gave a list of 22 primes $p \equiv 1 \pmod 9$, up to 2000, for which $C_p = 0$ i.e. (assuming BSD) p is a cube sum. Our computation yields this interesting observation that each of these primes is expressible as $f(x, y)$ for some $(x, y) \in \mathbb{Q}^2$. For example, $883 =$*

$f(\frac{14}{17}, \frac{195}{17})$. *Similarly, we have verified that all primes* $p \equiv 8 \pmod 9$, *up to* 500, *can be expressed as* $f(x, y)$ *for some* $(x, y) \in \mathbb{Q}^2$.

In Remark 2.5, we discuss density of the primes appearing in Theorem 2.4.

A variant of Corollary 2.11 is Corollary 2.10, where for any $d \in \mathbb{N}$ and for any integer a coprime to d, we show that there are infinitely many primes $p \equiv a^3 \pmod d$ such that each p is a rational cube sum. For example, Corollary 2.10 applies to $27 \pmod d$ whenever $3 \nmid d$ but it is not covered by Corollary 2.11.

In Prop. 3.16, we exhibit a certain family of primes p which are congruent to $1 \pmod 9$, and are values of f, such that we have $\text{rank}_{\mathbb{Z}}\ E_p(\mathbb{Q}) = 2$.

As a by-product of Theorem 2.4, we can show every non-zero equivalence class modulo a prime q contains infinitely many primes which are rational cube sums. This result establishes the complimentary case to the result of [4] stated in Theorem 1.1.

Theorem B (Theorem 2.9)**.** *Let* q *be a prime. Each residue class* $a \pmod q$, *for* $0 < a < q$, *contains infinitely many primes which are rational cube sums. These primes are obtained as values of the cubic form* $(X + Y)^3 - 9XY^2$ *at certain integer points.* □

Regarding the cube sum problem for a composite integer n, if n has more than one prime divisor, then results regarding expressibility of n as a rational cube sum are far more scarce. After the classical work of Sylvester, Satgé [3], [13] and others have typically considered integers of the form $p^i q^j$ where $i, j \leq 2$ and p, q are distinct primes with $p \in \{2, 3, 5\}$ and $q \equiv 2, 5 \pmod 9$. Using 3-descent on the Selmer group, some of these results were extended recently in [14] and [15].

Results regarding integers having 3 or more prime factors seem even scarcer and we are only aware of results in [16] which showed that for any odd integer $k \geq 1$, there exist infinitely many cube-free odd integers n with exactly k distinct prime factors such that $2n$ is a cube sum; similarly, there exist infinitely many cube-free odd integers n with exactly k distinct prime factors such that $2n$ is not a cube sum.

In this context, we have a very general result for an arbitrary integer N:

Theorem C (Theorem 3.6)**.** *For any integer* N, *there are infinitely many primes* p, *in each of the residue classes* $8 \pmod 9$ *and* $1 \pmod 9$, *so that* Np *is a rational cube sum. Each such prime* p *is a value of the cubic form* $X^3 + NY^3$ *at a certain integer point.* □

Further, for $N = \ell$ and $N = \ell^2$ i.e. integers of the form ℓp and $\ell^2 p$, where ℓ, p are primes, we strengthen Theorem 3.6 in Corollary 3.7, to include more congruence classes, in addition to $\pm 1 \pmod 9$. In particular, Corollary 3.7 applies to integers of the form $2p$ and $3p$ for a prime p. A variant of Corollary 3.7 appears in Proposition 3.21 where, using prime values of a different binary cubic form, we produce other infinite families of rational cube sums of the form ℓp and $\ell^2 p$ for certain primes ℓ and p.

A couple of reformulations of the rational cube sum problem, are given in Lemma 3.1 and Proposition 3.18. Lemma 3.1 is used in Theorem 3.6 and throughout §3.

Indeed, using Lemma 3.1, we generate many infinite families of composite integers that are rational cube sums, in Corollaries 3.9 -3.12. Moreover, we can show that (Prop. 3.4) given any integer k, there are infinitely many integers n such that both n and $n + k$ are rational cube sums.

Given any integer n, a natural question is whether $n = x^3 + y^3$ is solvable over certain quadratic fields. In Prop. 4.2, we show that any $n \in \mathbb{N}$ is a sum of two cubes over the infinite family of imaginary quadratic fields $\{\mathbb{Q}(\sqrt{-3(4nt^3 - 27)}) : t \in \mathbb{N}, t \geq 3\}$. Using a result of [17], we discuss a variant of this result in Prop 4.1. We also apply Proposition 4.2 to generate another infinite family of integers that are rational cube sums.

The article is structured as follows: In section 2, we discuss the rational cube sum problem for prime numbers. We write down two simple polynomial identities involving the binary cubic forms $(X + Y)^3 - 9XY^2$, $XY(X - Y)$ and use [11] to prove Theorems A and B. In section 3, we deduce that certain infinite families of composite numbers are rational cube sums. In particular, we prove Theorem C. The identities in Lemma 3.1 and 3.18 are important in §3.

In section 4, we discuss expressibility of $n \in \mathbb{N}$ as a sum of two cubes over imaginary quadratic fields. We remark that, although the method used in this article are quite simple, the results obtained here can perhaps be viewed as small steps in some classical problems that were open till date.

2 Cube sum prime numbers; Proofs of Theorem A and Theorem B

In this section, we discuss the rational cube sums problem for prime numbers in congruence classes and use [11, Theorem 1.1] to give the proofs of Theorems A and B. We begin by considering the following two binary cubics

$$f(X,Y) = (X+Y)^3 - 9XY^2 \qquad \text{and} \qquad g(X,Y) = XY(X-Y), \tag{1}$$

and the binary quadratic $h(X,Y) := X^2 - XY + Y^2$. Then, we have the following identity:

Proposition 2.1. *With $f(X,Y), g(X,Y), h(X,Y)$ as above, we have:*

$$\big(f(X,Y) - 3g(X,Y)\big)^3 + 27g(X,Y)^3 = f(X,Y)h(X,Y)^3. \tag{2}$$

$$f(X,Y)^3 - f(Y,X)^3 = 27g(X,Y)h(X,Y)^3. \tag{3}$$

In particular, $f(x,y)$ and $g(x,y)$ are sums of two rational cubes for all $(x,y) \in \mathbb{Q}^2$.

Proof. The proof follows from straightforward but tedious computation. Alternatively, one can easily validate these identities using any computer algebra system. □

Remark 2.2. *Let $(m,n) \in \mathbb{Q}^2$. Note that $m^3 + n^3 = (m+n)N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(m + n\zeta_3)$ and hence $m+n$ is a rational cube sum if $N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(m+n\zeta_3) \in \mathbb{Q}^3$. From this observation, we can alternatively deduce $f(x,y)$ is a rational cube sum for all $(x,y) \in \mathbb{Q}^2$. Indeed, put $m = x^3 + y^3 - 3xy^2$ and $n = 3xy(x-y)$, then $N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(m+n\zeta_3) \in \mathbb{Q}^3$.*

A similar computation will also prove $g(x,y)$ is a cube sum.

Remark 2.3. *A century old paper [18] mentions Ryley's formula which in which any $q \in \mathbb{Q}^\times$ can be written as sum of cubes of three rationals in infinitely many possible ways.*

As a simple application of (2), we re-prove this result. Let $q \in \mathbb{Q}^\times$. For any $r \in \mathbb{Q}^\times$, notice that $q = \big(r^2q + \frac{1}{3r}\big)^3 - \frac{1}{r^3} f\big(r^3q, \frac{1}{3}\big)$. Now from (2), $f\big(r^3q, \frac{1}{3}\big)$ is a sum of two rational cubes. Hence q is a sum of 3 rational cubes for every choice of $r \in \mathbb{Q}^\times$.

Heath-Brown and Moroz in [11] discuss the problem of representation of primes (with congruence condition) via integral binary cubic forms, extending results in [10] and [9]. Let $T(X,Y) \in \mathbb{Z}[X,Y]$ be an irreducible polynomial representing a binary cubic form. Let $a,b,d \in \mathbb{Z}$ such that $\mathfrak{T}(X,Y) := T(a+dX, b+dY)$ is a primitive polynomial and assume no prime divides all the values $\{\mathfrak{T}(x,y) \mid x,y \in \mathbb{Z}\}$. Then by [11, Theorem 1], $\mathfrak{T}(x,y)$ attains infinitely many prime values. Using this, we prove:

Theorem 2.4. *There are infinitely many primes p in each of the residue classes $1 \pmod 9$ and $8 \pmod 9$, such that p is a rational cube sum. Each of these primes p of the form $1 \pmod 9$ (respectively $8 \pmod 9$) is a value of the cubic form $f(X,Y) = (X+Y)^3 - 9XY^2$ at $(-1+3x, -1+3y)$ (respectively $(1+3x, 1+3y)$), for some $x,y \in \mathbb{Z}$.*

Proof. Set $f(X,Y) = (X+Y)^3 - 9XY^2$. Then $f(X,Y)$ is an irreducible polynomial in $\mathbb{Z}[X,Y]$. Put $\mathfrak{F}_\pm(X,Y) := f(\mp 1 + 3X, \mp 1 + 3Y)$. As $\mathfrak{F}_\pm(0,0) = \pm 1$, we see that $\mathfrak{F}_\pm(X,Y)$ are primitive polynomials in $\mathbb{Z}[X,Y]$ and no prime divides all the values $\{\mathfrak{F}_+(x,y) | x,y \in \mathbb{Z}\}$ (respectively $\{\mathfrak{F}_-(x,y) | x,y \in \mathbb{Z}\}$). Thus by [11, Theorem 1], there are infinitely many primes of the form $\mathfrak{F}_+(x,y)$ (respectively $\mathfrak{F}_-(x,y)$) for $(x,y) \in \mathbb{Z}^2$. Clearly, $\mathfrak{F}_\pm(x,y) \equiv \pm 1 \pmod 9$ for all $x,y \in \mathbb{Z}$. Now the statements follow from Proposition 2.1. □

Remark 2.5 (Density of primes). *It is evident that the density of primes appearing in each of the cases* $\pm 1 \pmod 9$ *in Theorem 2.4, is the same as the density obtained in [11, Theorem 1]. Let* $F \in \{-\mathfrak{F}_{\pm}\}$. *For* $X \gg 0$, *[11] considers a square* $I(X) = (X, X(1+\eta)] \times (X, X(1+\eta)]$, *where* $\eta = (\log X)^{-c} < 1$ *and* $\pi(F, X)$ *counts the number of primes of the form* $F(a,b)$ *for* $(a,b) \in I(X)$. *By [11, Theorem 2],* $\pi(F,X) = \sigma_1(F)\frac{\eta^2 X^2}{3\log X}\{1 + O((\log\log X)^{\frac{-1}{6}})\}$ *as* $X \to \infty$, *where* $\sigma_1(F)$ *is a positive constant, depending on* F.

Remark 2.6. *Numerical computations carried out by us indicate that number of distinct primes* p, *such that* $f(a,b) = p^2$ *for* $(a,b) \in [-X, X] \times [-X, X]$ *is of the order* $\frac{\sqrt{X}}{\log X}$, *and moreover roughly half of these primes are* 1 *modulo* 9 *and the other half of these primes are* -1 *modulo* 9. *However, to prove that a binary cubic form attains infinitely many prime square values, one has to obtain an analogue of the lower bound for the density obtained in the proof of [11, Theorem 2] using Sieve theory methods. But, we understand following some correspondences with Prof. Heath-Brown that proving such a result may be a difficult problem in Sieve theory.*

From Theorem 2.4, it follows that for $q = 2, 3$, the non-zero residue classes modulo q contain infinitely many primes that are rational cube sums. To establish this result for a general prime q, we begin with the following observation for $f(X,Y) = (X+Y)^3 - 9XY^2$:

Lemma 2.7. *Let* $q > 3$ *be a prime and let* $0 < a < q$ *be an integer. Then* $f(X,Y) = a$ *is a non-singular plane curve over* $\mathbb{F}_q$.

Proof. The curve is singular over $\mathbb{F}_q$ if and only if $\exists\ (\alpha,\beta) \in \mathbb{F}_q^2$ such that $f(\alpha,\beta) = a$ and the partial derivatives $f_X(\alpha,\beta) = f_Y(\alpha,\beta) = 0$. First of all, if $\alpha \in \mathbb{F}_q$ with $f(\alpha,0) = a$ i.e. $\alpha^3 = a$, then $f_X(\alpha,0) = f_Y(\alpha,0) = 3\alpha^2 \neq 0$. Thus, we can assume that $\beta \neq 0$. Then

$$f_X(\alpha,\beta) = 3\beta^2((\alpha/\beta+1)^2 - 3) \quad \text{and} \quad f_Y(\alpha,\beta) = 3\beta^2((\alpha/\beta-2)^2 - 3). \tag{4}$$

Thus it reduces to assume that $3 = \gamma^2$ for some $\gamma \in \mathbb{F}_q$. However, using $q > 3$ and $\beta \neq 0$, we get from (4) that $4\gamma^2 - 9 = 0$, which is a contradiction. □

Corollary 2.8. *Let* $q > 3$ *be a prime and* $0 < a < q$ *an integer. There exists* $(\alpha,\beta) \in \mathbb{F}_q^2$ *such that* $f(\alpha,\beta) = a$.

Proof. By Lemma 2.7, the cubic curve $f(X,Y) = aZ^3$ is non-singular. If $f(X,Y) - aZ^3$ is reducible, then there is a linear factor and hence there is a rational point $(\alpha,\beta) \in \mathbb{F}_q^2$ with $f(\alpha,\beta) = a$. On the other hand, if $f(X,Y) = aZ^3$ is irreducible, then it is a curve of genus 1, and hence it has $q + 1 - t$ rational points (including the point of infinity), where $|t| < 2\sqrt{q} < q$ (since $q \geq 5$). Thus, in either case, $\exists\ (\alpha,\beta) \in \mathbb{F}_q^2$ such that $f(\alpha,\beta) = a$. □

Now we are ready to prove Theorem B which is complimentary to the result of [4] (Theorem 1.1).

Theorem 2.9. *Let* $q > 3$ *be a prime and* $0 < a < q$ *an integer. Each residue class* $a \pmod q$ *contains infinitely many primes which are rational cube sums.*

Proof. By Corollary 2.8, there exists $(\alpha,\beta) \in \mathbb{F}_q^2$ so that $f(\alpha,\beta) = (\alpha+\beta)^3 - 9\alpha\beta^2 = a$. If $(k_1,k_2) \in \mathbb{Z}^2$ are such that $k_1 \equiv \alpha \pmod q$ and $k_2 \equiv \beta \pmod q$, then $f(k_1+qx, k_2+qy) \equiv a \pmod q$ for any $(x,y) \in \mathbb{Z}^2$. Recall $f(X,Y) \in \mathbb{Z}[X,Y]$ is irreducible and as $(a,q) = 1$, $\mathfrak{F}(X,Y) := f(k_1+qX, k_2+qY)$ is a primitive polynomial. Further $q \nmid \mathfrak{F}(0,0)$ and if there is a prime $p \neq q$ dividing all the values $\{\mathfrak{F}(m,n) \mid m,n \in \mathbb{Z}\}$, then we can find $c,d \in \mathbb{Z}$ satisfying $k_1 + qc \equiv 1 \pmod p$ and $k_2 + qd \equiv 0 \pmod p$. Then $\mathfrak{F}(c,d) \equiv 1 \pmod p$, which is a contradiction. Hence we can apply [11, Theorem 1] to deduce that there are infinitely many primes of the form $\mathfrak{F}(x,y)$ for $(x,y) \in \mathbb{Z}^2$ and by construction $\mathfrak{F}(x,y) \equiv a \pmod q$. Each of these primes are rational cube sums by Proposition 2.1. □

Following Theorems 2.4 and 2.9, one may ask the following more general question: Let d be a positive integer. When does the residue class $a \pmod d$ with $(a,d) = 1$, contain infinitely many primes (or contains no primes) which are rational cube sums?

One can imitate the proof above to show that if there exists $(k_1, k_2) \in \mathbb{Z}^2$ such that $f(k_1, k_2) \equiv a \pmod{d}$, then there are infinitely many primes $p \equiv a \pmod{d}$ which are rational cube sums. Observe that $f(k, k) = -k^3$ and hence, we deduce:

Corollary 2.10. *Let d be a positive integer and $(a, d) = 1$. If a is a cube modulo d, then the residue class $a \pmod{d}$ has infinitely many primes which are rational cube sums.*

Now we prove Theorem A which extends Theorem 2.4.

Corollary 2.11. *Let d be any positive integer. For any $a \in \mathbb{Z}$ with $(a, d) = 1$ and $a \equiv \pm 1 \pmod{9}$, there are infinitely many primes $p \equiv a \pmod{9d}$ which are rational cube sums.*

Proof. The proof is immediate from the following Lemma 2.12 and Proposition 2.1. □

Lemma 2.12 was communicated to us by Professor Heath-Brown.

Lemma 2.12. *Let $f(x, y) = (x+y)^3 - 9xy^2$. Suppose $a \equiv \pm 1 \pmod{9}$. Let d be any positive integer such that $(a, 9d) = 1$. Then, there exist integers r, s such that $f(r, s) \equiv a \pmod{9d}$. Further, there are infinitely many primes p satisfying $p \equiv a \pmod{9d}$ which are values of f.*

Proof. For the first statement, we prove it for prime power moduli and apply the Chinese remainder theorem. First, if $p \neq 3$ is a prime dividing d, then $f(r, s) \equiv a \pmod{p}$ has a solution in integers r, s by Corollary 2.8.

To obtain integers x, y such that $f(x, y) \equiv a \pmod{p^e}$ for $e > 1$, we apply Hensel's lemma. If $f(r, s) \equiv a \pmod{p}$, we show that the partial derivatives $f_x(r, s)$ and $f_y(r, s)$ are not both $0 \pmod{p}$. Indeed, $f_x = 3(x + y)^2 - 9y^2$; $f_y = 3(x + y)^2 - 18xy$. If $f_x(r, s) \equiv f_y(r, s) \equiv 0 \pmod{p}$ where $f(r, s) \equiv a \pmod{p}$, then we have

$$r f_x(r, s) + s f_y(r, s) = 3 f(r, s) \equiv 0 \pmod{p}$$

which is a contradiction. Therefore, Hensel's lemma applies to give a solution x, y for the congruence $f(x, y) \equiv a \pmod{p^e}$ for any $e \geq 1$.

Next, let $p = 3$; then it is easy to see (by induction) that $f(r, 0) = r^3 \equiv a \pmod{3^e}$ has solutions in integers r whenever $a \equiv \pm 1 \pmod{9}$. Observe that, writing $a = \pm 1 + 9k, k \in \mathbb{Z}$ it follows that $(\pm 1 + 3k)^3 \equiv \pm 1 + 9k \equiv a \pmod{3^3}$. Now for a general e, assume there exists a solution $r \in \mathbb{Z}$ of $r^3 \equiv a \pmod{3^{e-1}}$. Then using the 3-adic expansion of r, it is easy to get a solution $r_1 \equiv r \pmod{3^{e-1}}$ such that $r_1^3 \equiv a \pmod{3^e}$. Therefore, the first assertion is proved.

Now, if $f(r, s) \equiv a \pmod{9d}$, then consider $\mathfrak{F}(x, y) := f(r + 9dx, s + 9dy)$. As $(f(r, s), d) = 1$, $\mathfrak{F}$ is a primitive polynomial over $\mathbb{Z}$. Also there is no common prime divisor p of all the values of $\mathfrak{F}$. If such a prime exists, then $(p, 9d) = 1$ because $\mathfrak{F}(0, 0) \equiv a \pmod{9d}$ and $(a, 9d) = 1$. But, as before, we can solve for x_0, y_0 such that $r + 9dx_0 \equiv 1 \pmod{p}$ and $s + 9dy_0 \equiv 0 \pmod{p}$. Then, $\mathfrak{F}(x_0, y_0) \equiv f(1, 0) = 1 \pmod{p}$.

As $\mathfrak{F}$ is a primitive polynomial over $\mathbb{Z}$ and the values of $\mathfrak{F}$ has no common prime divisor, [11, Theorem 1.1] shows that $\mathfrak{F}(x, y)$ takes infinitely many prime values. □

3 Further polynomial identities and cube sum composite numbers

In this section, we generate several infinite families of composite integers that are rational cube sums. We repeatedly use the following reformulation of the cube sum problem. Although it seems to be known to experts, we write it down for the sake of completeness. Note that yet another reformulation appears in Prop. 3.18.

Lemma 3.1. *Any integer n of the form $n = xy(x - y)$ with $x, y \in \mathbb{Q}$ is a rational cube sum. Conversely, if a cube free integer $n \geq 2$ is a rational cube sum then $\exists\ x, y \in \mathbb{Q}$ such that $n = xy(x - y)$.*

Proof. The first assertion is immediate from the identity (3). The converse can be deduced using the fact that E_n is 3-isogenous to the curve $Y^2 = X^3 + 16n^2$ over $\mathbb{Q}$.

□

Remark 3.2. *In fact, as* $\mathrm{rk}_{\mathbb{Z}}\ E_n(\mathbb{Q}(\zeta_3)) = 2\ \mathrm{rk}_{\mathbb{Z}}\ E_n(\mathbb{Q})$*, we can also deduce:* $n \in \mathbb{Z}$ *is a rational cube sum* $\Leftrightarrow \exists\ x, y \in \mathbb{Q}(\zeta_3)$ *such that* $n = xy(x-y)$.

Example 3.3. *It is perhaps not obvious to express even a small number like* 42 *as a rational cube sum; using our identity* (3)*, we deduce* $g(-6,1) = 42 = (449/129)^3 + (-71/129)^3$.

We now discuss an interesting application of Lemma 3.1.

Proposition 3.4. *Given any integer* k*, there exists infinitely many pairs of integers* (m_i, n_i) *such that, for every* i*, both* m_i *and* n_i *are rational cube sums and* $m_i + n_i = k$.

In other words, given any integer k*, there are infinitely many integers* n *such that both* n *and* $n+k$ *are rational cube sums.*

Proof. We may assume $k \neq 0$. For each $i \geq 1$, put $(x_i, y_i) := \left(\frac{1}{2i} + 2i^2k, \frac{1}{2i} - 2i^2k\right)$. Then $g(x_i, y_i) = k - 16i^6k^3 = k - \left((2i^2k)^3 + (2i^2k)^3\right)$ is a rational cube sum. The result follows by defining $m_i = k - 16i^6k^3$ and $n_i = 16i^6k^3$. □

Remark 3.5. *For a fixed integer* $k \geq 0$*, let* $\pi_k(X) := \#\{n \in \mathbb{Z} : |n| \leq X$ *and both* $n, n+k$ *are rational cube sums}. [5, Theorem 1.1] implies that* $\pi_0(X) = O(X)$*. It will be interesting to study the asymptotic behaviour of* $\pi_k(X)$ *for* $k \geq 1$.

Using Lemma 3.1 and [11, Theorem 1], we are now ready to prove Theorem C.

Theorem 3.6. *For any integer* N *and for any* $(x, y) \in \mathbb{Z}^2$ *with* $xy \neq 0$*, the integer* $N(x^3 + Ny^3)$ *is a rational cube sum. In particular, for every* $n \in \mathbb{N}$*, there are infinitely many primes* p *in each of the residue classes* $1 \pmod 9$ *and* $8 \pmod 9$ *such that* Np *is a rational cube sum.*

Proof. From the identity $N(x^3+Ny^3) = \frac{1}{x^3}g(-Ny^3, x^3)$, we deduce that $N(x^3+Ny^3)$ is a rational cube sum. For the second part, if N is an integer cube then the result is a restatement of Theorem 2.4. On the other hand, if N is not a cube, then $T_N(X,Y) = X^3 + NY^3 \in \mathbb{Z}[X,Y]$ is an irreducible polynomial. Set $\mathfrak{T}_N(X,Y) := T_N(1+3X, 3Y)$. As $\mathfrak{T}_N(0,0) = 1$, we see that it is a primitive polynomial in $\mathbb{Z}[X,Y]$ and no prime divide all the values $\{\mathfrak{T}_N(x,y) | x, y \in \mathbb{Z}\}$. Thus by [11, Theorem 1], there are infinitely many primes p of the form $p = \mathfrak{T}_N(x,y)$, where x, y varies in $\mathbb{Z}$. Evidently, $\mathfrak{T}_N(x,y) \equiv 1 \pmod 9$. The result in the $8 \pmod 9$ case follows similarly, by considering $T_N(-1+3X, 3Y)$. □

The cube sum problem for $2p$ and $3p$, for a prime p are also stated as cases of Sylvester's Conjecture in the literature. We strengthen Theorem 3.6 for $N = 2, 3$ and, in fact, more generally for $N = \ell, \ell^2$ for a prime ℓ. The proofs follow a similar line of argument as in Theorem 3.6 using [11, Theorem 1]. We only give the specific input used in each case.

Corollary 3.7. *1. For each* $b \in \{1,4,7,8\}$*, there are infinitely many primes* $p \equiv b \pmod 9$ *such that* $3p$ *is a rational cube sum.*

2. Let $a \in \{1,2,7,8\}$ *and* ℓ *be a fixed prime so that* $\ell \equiv a \mod 9$*. Then for each* $b \in \{1,2,7,8\}$*, there are infinitely many primes* $p \equiv b \pmod 9$ *such that* ℓp *is a rational cube sum. In particular, for each* $b \in \{1,2,7,8\}$*, there are infinitely many primes* $p \equiv b \pmod 9$ *such that* $2p$ *is a rational cube sum.*

3. Let $a \in \{4,5\}$ *and* ℓ *be a fixed prime with* $\ell \equiv a \mod 9$*. For each* $b \in \{1,4,5,8\}$*, there are infinitely many primes* $p \equiv b \pmod 9$ *so that* ℓp *is a rational cube sum.*

4. Let $a \in \{1,4,5,8\}$*. Let* ℓ *be a fixed prime such that* $\ell \equiv a \mod 9$*. For each* $b \in \{1,2,7,8\}$*, there are infinitely many primes* $p \equiv b \pmod 9$ *such that* $\ell^2 p$ *is a rational cube sum.*

5. Let $\ell \equiv a \mod 9$ *be a fixed prime, where* $a \in \{2,7\}$*. For each* $b \in \{1,4,5,8\}$*, there are infinitely many primes* $p \equiv b \pmod 9$ *such that* $\ell^2 p$ *is a rational cube sum.*

Proof. First of all, for any ℓ or ℓ^2, the cases $b \in \{1,8\}$ directly follow from Theorem 3.6 and need not be argued again. We also make a general observation to be used in all the cases. Assume N is not an integer cube and take $a, b, \in \mathbb{Z}$. If $(a^3 + Nb^3, 3) = 1$, then $\mathfrak{T}(X,Y) := (a+3X)^3 + N(b+3Y)^3 \in \mathbb{Z}[X,Y]$ is a primitive polynomial. Next, if a prime q divides all the integer values of the primitive polynomial $\mathfrak{T}(X,Y)$, then by [11, Lemma 2.4], q can only be 2 or 3. Thus to conclude $\mathfrak{T}(X,Y)$

attains infinitely many prime values, it suffices to check (i) $3 \nmid a^3 + Nb^3 = \mathfrak{T}(0,0)$ and (ii) find $(c,d) \in \mathbb{Z}^2$ such that $2 \nmid \mathfrak{T}(c,d)$.

(1): For $b \equiv 4 \pmod 9$, put $\mathfrak{T}_3(X,Y) := T_3(1+3X, 1+3Y) \equiv 4 \pmod 9$. Note that $3 \nmid \mathfrak{T}_3(0,0) = 4$ and $\mathfrak{T}_3(1,0)$ is odd. For $b \equiv 7 \pmod 9$, consider $T_3(1+3X, -1+3Y)$.

(2) & (3): The proof follows from the three observations below.

(a) For any prime ℓ in case (2) or (3), set $\mathfrak{T}_\ell^{\pm}(X,Y) := T_\ell(3X, \pm 1 + 3Y) \equiv \pm\ell \pmod 9$. Note that $\mathfrak{T}_\ell^{\pm}(0,0) = \pm\ell$, is coprime to 3 and $\mathfrak{T}_\ell^{\pm}(1,1)$ is odd.

(b) For $\ell \equiv 1 \pmod 3$, consider $\mathcal{T}_\ell^{\pm}(X,Y) := T_\ell(\pm 1 + 3X, \pm 1 + 3Y) \equiv \pm(1+\ell) \pmod 9$ and notice that $3 \nmid \mathcal{T}_\ell^{\pm}(0,0) = \pm(1+\ell)$ and $\mathcal{T}_\ell^{\pm}(0,1)$ is odd.

(c) Finally, for $\ell \equiv 2 \pmod 3$, set $\widetilde{\mathcal{T}}_\ell^{\pm}(X,Y) := T_\ell(\mp 1 + 3X, \pm 1 + 3Y) \equiv \pm(-1+\ell) \pmod 9$ and observe that $3 \nmid \widetilde{\mathcal{T}}_\ell^{\pm}(0,0) = \pm(-1+\ell)$ and $2 \nmid \widetilde{\mathcal{T}}_\ell^{\pm}(0,1)$.

(4) & (5): The proof follows from similar observations as in the case (a) and (b) above. For any ℓ appearing in case (4) or (5), put $\mathfrak{T}_{\ell^2}^{\pm}(X,Y) := T_{\ell^2}(3X, \pm 1 + 3Y) \equiv \pm\ell^2 \pmod 9$. Then $3 \nmid \mathfrak{T}_\ell^{\pm}(0,0) = \pm\ell^2$ and $\mathfrak{T}_\ell^{\pm}(1,0)$ is odd. Next, set $\mathcal{T}_{\ell^2}^{\pm}(X,Y) := T_{\ell^2}(\pm 1 + 3X, \pm 1 + 3Y) \equiv \pm(1+\ell^2) \pmod 9$ and notice that $3 \nmid \mathcal{T}_\ell^{\pm}(0,0) = \pm(\ell^2+1)$ and $2 \nmid \mathcal{T}_\ell^{\pm}(0,1)$. □

Remark 3.8 (Related works)**.** *Note that in Theorem 3.6 and Corollary 3.7, we had $p = a^3 + Nb^3$, for some $a, b \in \mathbb{Z}$ i.e. N is a cube in $\mathbb{F}_p$. On the other hand, for any prime $p \equiv 1, 7 \pmod 9$ so that 2 is not a cube in $\mathbb{F}_p$, it is shown in [14, Corollary 5.9] that $2p$ is not a rational cube sum. For any prime $p \equiv 2 \pmod 9$, it was shown in [3] that $2p$ is a cube sum. However, if $p \equiv 5 \pmod 9$, then $2p$ is a not cube sum [1]. Recently, it was shown in [13] that for any prime $p \equiv 2, 5 \pmod 9$, $3p$ and also $3p^2$ are cube sums.*

Next, we draw several other corollaries of the Lemma 3.1. We state them separately simply because each has a different flavour.

Corollary 3.9. *Let $a, b \in \mathbb{Z}$. Notice that $g(a,b) = 2(a-b)\frac{a}{2}b$, i.e. $g(a,b)$ is twice the product of 3 rational numbers in arithmetic progression (AP). Conversely, given 3 rationals $a, a+d$ and $a+2d$ in AP, we get $2a(a+d)(a+2d) = g(2a+2d, a+2d)$. Thus a cube-free integer $n > 1$ is a rational cube sum $\Leftrightarrow$ n is twice the product of three rational numbers in AP. In particular, $2n(n+k)(n+2k)$ is a rational cube sum for arbitrary $n, k \in \mathbb{Z}$.*

Corollary 3.10. *For any pair of integers r, s, the numbers $g(r,s) = rs(r-s)$ and $g(-r,s) = rs(r+s)$ are rational cube sums. In particular,*

1. *The product of any two consecutive integers is a rational cube sum. Equivalently, for any matrix $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, $abcd$ is a rational cube sum.*
2. *For $x, y \in \mathbb{Z}$, $xy(x^{3k+1} \pm y^{3k+1}) = g(\mp x^{3k+1}, y^{3k+1})$ are rational cube sums. In particular, for any $(n,k) \in \mathbb{N}^2$, $n^{3k+2} \pm n$ are rational cube sums.*
3. *Given any three integers a, b, c, the integer $(a-b)(b-c)(c-a) = g(b-a, b-c)$ is a rational cube sum.*
4. *For any $n, k \in \mathbb{Z}$, $n(n+k)(2n+k) = g(-n, n+k)$ is a rational cube sum. In particular, for any $n \in \mathbb{Z}$, $2n(n+2)$ is a rational cube sum.*
5. *For any $d, k \in \mathbb{Z}$, $2d(d^2 - k^2) = g(-d-k, d-k)$ is a rational cube sum.*
6. *If $(x,y) \in \mathbb{Z}^2$ satisfies the Pell's equation $X^2 - NY^2 = 1$, then $Nx^2y^2 = g(x^2, 1)$ is a rational cube sum.*
7. *If ABC is a rational right angle triangle whose sides have lengths $a, b, c \in \mathbb{Q}$ respectively, then $(abc)^2$ is a rational cube sum.*
8. *As a special case of Corollary 3.9, $2n(n+1)(n+2) = g(2n+2, n+2)$ is a rational cube sum. It is the area of an isosceles Heron triangle whose sides have lengths $n^2 + 2n + 2, n^2 + 2n + 2$ and $2(n^2 + 2n)$.*

9. *Integers of the form $n = d(8d+1), d \in \mathbb{Z}$ are rational cube sums. In particular, for any integer k, $\frac{1}{2}k(k+1)(2k+1)^2$ is a rational cube sum.*
10. *For any integer n, n^2-16, $3n^2+16$ and n^2+432 are rational cube sums. More generally, integers of the form $(4T^3)2+3V^2$ and $\frac{1}{4}(L^2+27(M^3)^2)$ are rational cube sums.*
11. *If the polynomial $T(X) = aX^2 - bX + c \in \mathbb{Z}[X]$ has a root in $\mathbb{Q}(\zeta_3)$, then abc is a rational cube sum.*

Proof. We give a brief justification of (9), (10) and (11).

(9) We have $g(a^3+b^3d, a^3) = (ab)^3(a^3d+b^3d^2)$ and hence integers of the form $a^3d+b^3d^2$ are rational cube sums. In particular, $g(1+8d, 1) = 2^3d(8d+1)$.

(10) Observe that $g(n+4, n-4) = 8(n^2-16)$ and hence n^2-16 is a rational cube sum. On the other hand, $g(V\sqrt{-3}+4T^3, V\sqrt{-3}-4T^3) = -8T^3(3V^2+16T^6)$, and hence $(4T^3)^2+3V^2$ is a rational cube sum by Remark 3.2. Similarly, $\frac{(M\sqrt{-3})^3}{4}(L^2+27(M^3)^2) = g(\frac{L-3\sqrt{-3}M^3}{2}, \frac{L+3\sqrt{-3}M^3}{2})$.

(11) Let $\alpha, \beta \in \mathbb{Q}(\zeta_3)$ be the roots of $T(X)$, then $abc = a^3g(-\alpha, \beta)$. The result then follows from Remark 3.2.

□

Let F_n (resp. L_n) denote the n^{th} term of the Fibonacci Sequence (resp. Lucas number); the convention here is $F_0 = 0, F_1 = 1, L_0 = 2, L_1 = 1$.

Corollary 3.11. *A product of the three consecutive terms in the Fibonacci sequence (respectively, three consecutive Lucas numbers) is a rational cube sum.*

Proof. We have $F_nF_{n+1}F_{n+2} = g(F_{n+2}, F_{n+1})$ and $L_nL_{n+1}L_{n+2} = g(L_{n+2}, L_{n+1})$. □

Using identities for Fibonacci and Lucas sequences, one can write down many such formulae. For example, each of the following products are rational cube sums by Lemma 3.1: $F_{n-1}L_nF_{n+1} = g(L_n, F_{n+1})$, $F_{n-1}^2F_{n+1}^2F_{2n} = g(F_{n+1}^2, F_{n-1}^2)$,
$F_{n-1}F_n^2F_{n+1} = (-1)^{n-1}g(F_n^2, F_{n-1}F_{n+1})$, $5L_{n-1}L_n^2L_{n+1} = (-1)^n g(L_n^2, L_{n-1}L_{n+1})$.

Corollary 3.12. *One can take an elliptic curve E with infinitely many rational points $P = (x(P), y(P))$. Then applying suitable polynomials like $f(X,Y)$, $g(X,Y)$ (1) on P will give rise to families of integers (after clearing denominators) which are rational cube sums. We illustrate this with a couple of examples:*
(I) Consider the elliptic curve $E : y^2 = x^3 + 9$. Note that $(3,6) \in E(\mathbb{Q})$ is a non-torsion point. Now take $P = (x(P), y(P)) \in E(\mathbb{Q})$ to be any point of infinite order and write $y(P) = a/b$ with $(a,b) = 1$. Then $2a$ is a rational cube sum.

Indeed, for any prime p, $v_p(y(P)) < 0$ implies $v_p(y(P)) \equiv 0 \pmod 3$. Now by Corollary 3.10(5), we get $2y(P)x(P)^3 = 2y(P)(y(P)^2 - 9)$ is a rational cube sum.

(II) Consider the curve $E : y^2 = x^3 - 9x + 9$ with an infinite order point $(1,1) \in E(\mathbb{Q})$. Let $P = (x(P), y(P)) \in E(\mathbb{Q})$ be any non-torsion point. Then writing $y(P) = a/b$ with $(a,b) = 1$, we obtain a^2 is a cube sum using the identity $f(x(P)-1, 1) = y(P)^2$.

To generate more integers which are rational cube sums, we shall generalize the identities (2) and (3) to the identity (6) in Prop. (3.13). To do this, inspired by ideas from [12], we define a pair of binary cubics as follows:

$$f(X,Y) = (X+Y)^3 - 9XY^2 \quad \text{and} \quad f_1(X,Y) = f(X,Y) - 6g(X,Y) = X^3 + Y^3 - 3X^2Y. \tag{5}$$

The pair satisfies the following identity:

Lemma 3.13. *Let $(f(X,Y), f_1(X,Y))$ be the binary cubics as defined in (5) and recall $h(X,Y) = X^2 - XY + Y^2$. We have the following identity in $\mathbb{Z}[X,Y,Z,W]$:*

$$\begin{aligned} &\Big[\big((Zf(X,Y) + 3Wf_1(X,Y)\big) + \big((Zf_1(X,Y) - Wf(X,Y)\big)\Big]^3 + \\ &\Big[\big((Zf(X,Y) + 3Wf_1(X,Y)\big) - \big((Zf_1(X,Y) - Wf(X,Y)\big)\Big]^3 \\ &\qquad = (Z^2+3W^2)\big((Zf(X,Y) + 3Wf_1(X,Y)\big)(2h(X,Y))^3. \end{aligned} \tag{6}$$

Proof. We have the following identity.

$$f(X,Y)^2 + 3f_1(X,Y)^2 = 4h(X,Y)^3, \tag{7}$$

which can be verified via straightforward, but tedious, computation. Using (7) and the identities $(a^2+3b^2)(c^2+3d^2) = (ac+3bd)^2+3(ad-bc)^2$ and $(a+b)^3+(a-b)^3 = 2a(a^2+3b^2)$, the identity in (6) can be deduced. Alternatively, (6) can be validated using any computer algebra system. □

Note that the result in Proposition (2.1) can be recovered from the identity (6). Indeed, by putting $Z = 1, W = 0$ (respectively $Z = 3, W = -1$) in the identity (6), we deduce $f(x,y)$ (respectively $g(x,y)$) are rational cube sums $\forall\ x, y \in \mathbb{Q}$.

As an immediate consequence of equation (6), we obtain:

Corollary 3.14. *Let n be an integer expressible as $n = u^2+3v^2$ for some $(u,v) \in \mathbb{Z}^2$. If there exist $(z,w) \in \mathbb{Q}^2$ such that $uf(z,w)+3vf_1(z,w) = 1$, then n is a cube sum.*

Remark 3.15. *Recall that a prime $p \equiv 1 \pmod 3$ can be written as $p = u^2+3v^2$ for some $(u,v) \in \mathbb{Z}^2$. For all primes $p < 500$, such that $p \equiv 4, 7 \pmod 9$ and 2 is not a cube modulo p, we have verified that there exist $(u,v) \in \mathbb{Z}^2$ and $(z,w) \in \mathbb{Q}^2$ such that $u^2+3v^2 = p$ and $uf(z,w)+3vf_1(z,w) = 1$. Thus all of these primes are cube sums by Lemma 3.14. Note that, for some of these primes (for example 31), 3 is a cube mod p.*

Recall, for a prime $p \equiv 1 \pmod 9$, the root number of $E_p : y^2 = X^3 - 432p^2$ is 1 and by a 3-descent argument, one can check $\operatorname{rank}_{\mathbb{Z}} E_p(\mathbb{Q}) \leq 2$. Thus assuming the parity conjecture, the rank of $E_p(\mathbb{Q})$ is 0 or 2. We now show (without any assumption on the BSD conjecture or the parity conjecture) that for a certain family of primes $p \equiv 1 \pmod 9$, the Mordell-Weil ranks of $E_p(\mathbb{Q})$ and $E_{p^2}(\mathbb{Q})$ equals 2.

Proposition 3.16. *Let $p \equiv 1 \pmod 9$ be a prime and put $p' \in \{p, p^2\}$. Let $(u,v) \in \mathbb{Z}^2$ such that $p' = u^2+3v^2$. Assume both the following conditions hold:*

1. *There exists rational numbers $(x,y) \in \mathbb{Q}^2$ such that $f(x,y) = p'$.*
2. *There exists rational numbers $(z,w) \in \mathbb{Q}^2$ such that $uf(z,w)+3vf_1(z,w) = 1$.*

Then $\operatorname{rk}_{\mathbb{Z}} E_{p'}(\mathbb{Q}) = 2$ and the 3-part of the Tate-Shafarevich group $Ш(E_{p'}/\mathbb{Q})[3]$ vanishes.

Proof. We prove the result for p and the proof for p^2 is similar. We know that $E_p(\mathbb{Q})_{\text{tor}} = 0$ and using a 3-descent argument (for example [14, §5]), one can show for the 3-Selmer group of E_p over $\mathbb{Q}$, $\dim_{\mathbb{F}_3} S_3(E_p/\mathbb{Q}) \leq 2$. We will show that $\dim_{\mathbb{F}_3} E_p(\mathbb{Q})/3E_p(\mathbb{Q}) \geq 2$. Hence $\operatorname{rk}_{\mathbb{Z}} E_p(\mathbb{Q}) = 2$ and $Ш(E_p/\mathbb{Q})[3] = 0$ follows from the descent exact sequence $0 \to E_p(\mathbb{Q})/3E_p(\mathbb{Q}) \to S_3(E_p/\mathbb{Q}) \to Ш(E_p/\mathbb{Q})[3] \to 0$.

Recall that if $X^3+Y^3 = p$, then $\left(\frac{12p}{X+Y}, 36p\frac{X-Y}{X+Y}\right) \in E_p(\mathbb{Q})$. By condition (1), it follows from (2) that $P := \big(12h(x,y), 36f_1(x,y)\big) \in E_p(\mathbb{Q})$. Further using hypothesis (2), from the identity (6), it follows that $Q := \big(12ph(z,w), 36p[uf_1(z,w) - vf(z,w)]\big) \in E_p(\mathbb{Q})$. Also recall that for a non-trivial rational point $(x,y) \in E_p(\mathbb{Q})$, the Kummer map $\delta : E_p(\mathbb{Q}) \to \mathbb{Q}(\zeta_3)^*/\mathbb{Q}(\zeta_3)^{*3}$ is given by $\delta\big((x,y)\big) = y - 12p\sqrt{-3}$ (for example, see [14, §3]). It follows that $\delta(P) = \zeta_3^2$ and $\delta(Q) = \zeta_3^2\pi_p^2\overline{\pi}_p$, where $\zeta = \frac{-1+\sqrt{-3}}{2}$ and $\pi_p = u+\sqrt{-3}v$. As a consequence, it follows that $\delta(P), \delta(Q), \delta(P+Q)$ and $\delta(P-Q)$ are all non-trivial elements in $\mathbb{Q}(\zeta_3)^*/\mathbb{Q}(\zeta_3)^{*3}$. Hence $[P], [Q], [P+Q]$ and $[P-Q]$ are non-trivial in $E_p(\mathbb{Q})/3E_p(\mathbb{Q})$, which in turn implies that $\dim_{\mathbb{F}_3} E_p(\mathbb{Q})/3E_p(\mathbb{Q}) = 2$. □

Remark 3.17. *One may wonder how often both the conditions in Prop. 3.16 hold. In [8], assuming BSD, it is shown that there are 22 primes $p \equiv 1 \pmod 9$, $p < 2000$ for which $\operatorname{rk}_{\mathbb{Z}} E_p(\mathbb{Q}) = 2$. We have verified via SAGE that both the conditions are satisfied by all those 22 primes.*

Next, we consider the following homogeneous reducible polynomial in 4 variables.

$$p_f(X,Y,Z,W) = (Z^2+3W^2)\big[Zf(X,Y)+3Wf_1(X,Y)\big], \tag{8}$$

Proposition 3.18. *For $(a,b,u,v) \in \mathbb{Q}^4$, the rational number $p_f(a,b,u,v)$ is a rational cube sum. Conversely, if $n \in \mathbb{Z}$ is a rational cube sum, then for any $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$, there exists $(u,v) \in \mathbb{Q}^2$ such that $n = p_f(a,b,u,v)$.*

Proof. Observe that $p_f(0,0,u,v) = 0$ for any $(u,v) \in \mathbb{Q}^2$ and thus, we may assume $(a,b) \neq (0,0)$. Consider the rational numbers $\alpha_f = \alpha_f(a,b) = \frac{f(a,b)+f_1(a,b)}{2h(a,b)}$, $\beta_f = \beta_f(a,b) = \frac{3f_1(a,b)-f(a,b)}{2h(a,b)}$, $\gamma_f = \gamma_f(a,b) = \frac{f(a,b)-f_1(a,b)}{2h(a,b)}$ and $\delta_f = \delta_f(a,b) = \frac{3f_1(a,b)+f(a,b)}{2h(a,b)}$. Then it is immediate from (6) that

$$p_f(a,b,u,v) = (u\alpha_f + v\beta_f)^3 + (u\gamma_f + v\delta_f)^3,$$

is a rational cube sum. It follows that for any fixed $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$, $p_f(a,b,Z,W) = \big(\alpha_f Z + \beta_f W\big)^3 + \big(\gamma_f Z + \delta_f W\big)^3$, with $\alpha_f\delta_f - \beta_f\gamma_f = 2h(a,b) \neq 0$. Now given an integer $n = c^3 + d^3$ with $c,d \in \mathbb{Q}$, observe that $p_f\big(a,b,\frac{\delta_f c - \beta_f d}{\alpha_f\delta_f - \beta_f\gamma_f}, \frac{-\gamma_f c + \alpha_f d}{\alpha_f\delta_f - \beta_f\gamma_f}\big) = c^3 + d^3$. □

We illustrate Proposition 3.18 via an example; one can construct many other examples for various choices of (a,b).

Corollary 3.19. *Taking $(a,b) = (1,0)$, we obtain an integer n is a rational cube sum $\Leftrightarrow n = (z^2+3w^2)(z+3w)$ for some $(z,w) \in \mathbb{Q}^2$.*

Now we consider a special case of Theorem 3.6 for $N = 9$ and produce a different family of infinitely many primes, in each of the classes $\pm 1 \pmod 9$ such that $9p$ is a cube sum.

Corollary 3.20. *There are infinitely many primes p (of the form $p = c^3+d^3-3c^2d$ with $c,d \in \mathbb{Z}$), in each of the residue classes $1 \pmod 9$ and $8 \pmod 9$ such that $9p$ is a rational cube sum.*

Proof. For $a,b \in \mathbb{Z}, 9(a^3+b^3-3a^2b) = p_f(a,b,0,1)$ is a rational cube sum (Prop. 3.18). Now $X^3+Y^3-3X^2Y \in \mathbb{Z}[X,Y]$ is irreducible, and applying [11, Theorem 1] and following the proof of Theorem 3.6, we deduce the result. □

Now we produce infinite families of integers with exactly two distinct prime factors that are rational cube sums. These results are variants of Theorem 3.6; however the infinite family of primes that appear in Prop. 3.21 are values of different binary cubic forms.

Proposition 3.21. *Let $p \equiv 1 \pmod 3$ be any prime. Let us choose $u,v \in \mathbb{Z}$ such that $u \equiv 1 \pmod 3$ and $u^2+3v^2 = p$.*

1. *There are infinitely many primes q in each of the residue classes $(u+3v) \pmod 9$ as well as $-(u+3v) \pmod 9$, such that the integers pq are rational cube sums.*
2. *There are infinitely many primes q in each of the residue classes $u^2+3v(2u-v) \pmod 9$ as well as $-u^2-3v(2u-v) \pmod 9$ such that p^2q are rational cube sums.*

Proof. (1) Set $q(X,Y) := (u+3v)[X^3+Y^3] + 3(u-3v)X^2Y - 6uXY^2$. As p is odd, $u \pm 3v$ are odd and by an elementary argument, we can deduce that $q(X,Y) \in \mathbb{Z}[X,Y]$ is irreducible. Set $\mathfrak{Q}(X,Y) := q(-u+3X, -u+3Y)$. Then

$$\mathfrak{Q}(X,Y) = 27(u+3v)[X^3+Y^3] + 81(u-3v)X^2Y + \cdots + u^3(u+3v).$$

As $(u,3v) = 1$, it is immediate that $\mathfrak{Q}(X,Y)$ is a primitive polynomial in $\mathbb{Z}[X,Y]$. By [11, Lemma 2.4], only possibility for a prime ℓ that divides all the values $\{\mathfrak{Q}(a,b) \mid a,b \in \mathbb{Z}\}$ is $\ell = 2$ or $\ell = 3$. Now $3 \nmid \mathfrak{Q}(0,0) = u^3(u+3v)$ and we can write $\mathfrak{Q}(0,1) = 81v + uT(u,v)$, for some $T(X,Y) \in \mathbb{Z}[X,Y]$. Further, both $\mathfrak{Q}(0,0)$ and $\mathfrak{Q}(0,1)$ can not be even. Hence the conditions of [11, Theorem 1] are met and hence there are infinitely many primes q of the form $q = \mathfrak{Q}(a,b)$ with a,b varying in $\mathbb{Z}$. It is clear that $\mathfrak{Q}(a,b) \equiv u+3v \pmod 9$ for any $a,b \in \mathbb{Z}$. Now, it is plain from (8) that $p_f(x,y,u,v) = pq(x,y)$ and thus by Prop. 3.18, $pq(x,y)$ is a rational cube sum for any $x,y \in \mathbb{Z}$. For the $-(u+3v) \pmod 9$ case, consider the polynomial $q(u+3X, u+3Y)$.

(2) Set $\ell(X,Y) := (u^2+6uv-3v^2)[X^3+Y^3]+3(u^2-6uv-3v^2)X^2Y-6(u^2-3v^2)XY^2$. As p is odd, $(u^2-3v^2)+2uv$ is odd and again by an elementary argument, we can see $\ell(X,Y) \in \mathbb{Z}[X,Y]$ is irreducible. Set $\mathfrak{L}(X,Y) := \ell(-1+3X,-1+3Y) = 27(u^2+6uv-3v^2)(X^3+Y^3)+81(u^2-6uv-3v^2)X^2Y+\cdots+27(u^2+6uv-3v^2)$. As $(u,v)=1$, we deduce that $\mathfrak{L}(X,Y)$ is primitive and also easy to see that $2,3 \nmid \mathfrak{L}(0,0)$. Then by [11, Theorem 1], there are infinitely many primes q which are integer values of $\mathfrak{L}$. Further $\mathfrak{L}(a,b) \equiv u^2 \pm 3v(2u-v) \pmod 9$, for any $a,b \in \mathbb{Z}$. Again from (8), we obtain $p_f(x,y,u^2-3v^2,2uv) = p^2\ell(x,y)$ and via Prop. 3.18, $p^2\ell(x,y)$ is a rational cube sum for any $x,y \in \mathbb{Z}$.
The other case follows by studying the polynomial $\ell(1+3X,1+3Y)$. □

Example 3.22. *From the proof of Proposition 3.21 it follows that for $(u,v) \in \mathbb{Z}^2$, if there exists $(x_0,y_0) \in \mathbb{Q}^2$ such that $uf(x_0,y_0)+3vf_1(x_0,y_0)=1$, then u^2+3v^2 is a rational cube sum. For example, taking $u=7,v=-2$, we note that $7f(1,0)-6f_1(1,0)=1$ and hence 61 is a rational cube sum. Note that $61 \equiv 7 \pmod 9$ and 3 is cube modulo 61, thus the fact that 61 is a rational cube sum does not follow from the results of [6].*

We now give an application of Proposition 3.21 to cubic reciprocity. Recall for a prime $p \equiv 1 \pmod 3$, 2 is a cube in $\mathbb{F}_p \Leftrightarrow p = u^2+27v^2$ for some $u,v \in \mathbb{Z}$.

Corollary 3.23. *Let $p \equiv 1 \pmod 3$ be any prime so that 2 is not a cube in $\mathbb{F}_p$. Choose $u,v \in \mathbb{Z}$ such that $p=u^2+3v^2$, $u \equiv 1 \pmod 3$ and $v \equiv 2 \pmod 3$.*

1. *Any prime $q \equiv 6-u \pmod 9 \equiv 2 \pmod 3$ of the form $q=(u-3v)x^3+3(u+3v)x^2y-6uxy^2+(u-3v)y^3$, $x,y \in \mathbb{Z}$, is a cube in $\mathbb{F}_p$. There are infinitely many such primes.*
2. *Any prime $q \equiv -u^2 \pmod 9 \equiv 2 \pmod 3$ of the form $(u^2+6uv-3v^2)x^3+3(u^2-6uv-3v^2)x^2y-6(u^2-3v^2)xy^2+(u^2+6uv-3v^2)y^3$, $x,y \in \mathbb{Z}$, is a cube in $\mathbb{F}_p$. There are infinitely many such primes.*

Proof. (1) Applying Proposition 3.21(1) for the pair $(u,-v)$, there are infinitely many primes q of the above mentioned form with $q \equiv -(u+3(-v)) \equiv 6-u \pmod 9$ such that the integers pq are rational cube sum. Observe that, in this setting, $pq \equiv 2 \pmod 9$. If q is not a cube in $\mathbb{F}_p$, then by a 3-descent argument [15, Theorem 3.1(3)], pq can not be a rational cube sum, which is a contradiction. Thus, q must be a cube in $\mathbb{F}_p$.

(2) Applying Proposition 3.21(2), there are infinitely many primes q of the above mentioned form with $q \equiv -u^2-3v(2u-v) \equiv -u^2 \pmod 9$, such that each of p^2q is a rational cube sum. Under this setting, $p^2q \equiv 2 \pmod 9$. Again, if q is not a cube $\pmod p$, then by [15, Theorem 3.1(3)], p^2q is not a rational cube sum, a contradiction. Thus, q must be a cube modulo p. □

4 Cube sums over imaginary quadratic fields

We say $n \in \mathbb{N}$ is a cube sum over a number field F if $n=x^3+y^3$ with $x,y \in F$. We discuss expressibility of an integer as a cube sum over imaginary quadratic fields.

Recall, E_n denotes the elliptic curve $y^2=x^3-432n^2$. For any prime p, let $Ш(E_n/\mathbb{Q})[p^\infty]$ denote the p-primary torsion part of the Tate-Shafarevich group of $E_n/\mathbb{Q}$ and let $S_{p^\infty}(E_n/\mathbb{Q})$ be the p^∞-Selmer group of $E_n/\mathbb{Q}$. Firstly, we show, under an assumption on $Ш(E_n/\mathbb{Q})[p^\infty]$, that $n \in \mathbb{N}$ is a cube sum over infinitely many imaginary quadratic fields.

Proposition 4.1. *Let n be any positive integer. Assume that $Ш(E_n/\mathbb{Q})[p^\infty]$ is finite for some prime $p \geq 5$, where $E_n : y^2=x^3-432n^2$. Then there are infinitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{-D_n})$ such that n is a cube sum over $\mathbb{Q}(\sqrt{-D_n})$, for each D_n.*

Proof. We may assume that n is not a cube sum over $\mathbb{Q}$. (In particular, $n>2$.) Then $E_n(\mathbb{Q})$ is finite. (By assumption,) choose a prime $p>3$ such that $Ш(E_n/\mathbb{Q})[p^\infty]$ is finite. Then the p^∞-Selmer group $S_{p^\infty}(E_n/\mathbb{Q})$ is finite. Now E_n has CM by $\mathbb{Q}(\zeta_3)$ and $p \nmid \#O^\times_{\mathbb{Q}(\zeta_3)}$, it follows from Rubin's work [19] on the Iwasawa main conjecture for imaginary quadratic fields that the complex L-value $L(E_n/\mathbb{Q},1) \neq 0$. Further, by results of Bump-Friedberg-Hoffstein, or Murty-Murty [17,

Corollary to Theorem 2], there are infinitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{-D_n})$ such that for the quadratic twists $E_n^{D_n}$ of E_n, the L-functions $L(E_n^{D_n}/\mathbb{Q}, s)$ have a simple zero at $s = 1$. Then it is known, by the Gross-Zagier theorem together with Kolyvagin's or Rubin's result that for any such D_n, the Mordell-Weil rank of $E_n^{D_n}(\mathbb{Q})$ is 1. Thus we get that $\text{rank}_{\mathbb{Z}}\ E_n(\mathbb{Q}(\sqrt{-D_n})) = 1$ as well and consequently n is a cube sum over $\mathbb{Q}(\sqrt{-D_n})$ for each of those D_n's. □

Now, using certain binary cubic forms, we give an explicit and unconditional construction of infinitely many imaginary quadratic fields over which n can be expressed as a cube sum.

Proposition 4.2. *Let n be any positive integer. For every integer $t \geq 3$, n is a cube sum over the imaginary quadratic field $K_{n,t} = \mathbb{Q}\big(\sqrt{-3(4nt^3 - 27)}\big)$.*

Proof. We construct an explicit binary cubic form and then make use of the strategy outlined by Mordell, Evertse (cf. [20, §3]). For any binary cubic form $F(X, Y)$, recall that the 'quadratic covariant' $H(x, y) := -\frac{1}{4}\left(\frac{\partial^2 F}{\partial X^2}\frac{\partial^2 F}{\partial X^2} - (\frac{\partial^2 F}{\partial X \partial Y})^2\right)$ has the discriminant $= -3D$, where D is the discriminant of F. Further, if we set the 'cubic covariant' $G(x, y) := \frac{\partial F}{\partial X}\frac{\partial H}{\partial Y} - \frac{\partial F}{\partial Y}\frac{\partial H}{\partial X}$, then one has $4H(X, Y)^3 = G(X, Y)^2 + 27DF(X, Y)^2$.

For any positive integer t, consider the binary cubic form $f_{n,t}(X, Y) = (X + Y)^3 - nt^3XY^2$. It is easy to see that $f_{n,t}(X, Y) \in \mathbb{Z}[X, Y]$ is an irreducible polynomial for $t > 2$.

We compute in this case $D = D(f_{n,t}) = (nt^3)^2(4k^3n - 27)$ and thus for any given n and for every choice of $t > 2$, the discriminant $D(f_{n,t})$ is positive. Setting $K_{n,t} := \mathbb{Q}(\sqrt{-3D}) = \mathbb{Q}(\sqrt{-3(4nt^3 - 27)})$, it follows that $f_{n,t}(X, Y)$ is an irreducible polynomial in $K_{n,t}[X, Y]$ as well [20, Page 122]. Further, put $U^{\pm}_{n,t}(X, Y) = \frac{1}{2}(G_{n,t}(x, y) \pm 3\sqrt{-3D}F_{n,t}(X, Y))$. Then we get $U^{+}_{n,t}(X, Y)U^{-}_{n,t}(X, Y) = H_{n,t}(X, Y)^3$ [20, Eq. 10]. As $U^{+}_{n,t}(X, Y)$ and $U^{-}_{n,t}(X, Y)$ have no common factors, it follows that each of them is a cube of some homogeneous linear forms $\xi^{\pm}_{n,t}(X, Y) \in K_{n,t}[X, Y]$, respectively. One obtains that $G_{n,t}(X, Y) = \xi^{+}_{n,t}(X, Y)^3 + \xi^{-}_{n,t}(X, Y)^3$ [20, Eq. 11].

Observe that $G_{n,t}(1, 0) = -27nk^3$. Thus any given $n \in \mathbb{N}$ is a cube sum over the imaginary quadratic field $\mathbb{Q}(\sqrt{-3(4nt^3 - 27)})$ for every choice of $t \geq 3$. □

Remark 4.3. *Note that, for any positive integer n, $K_{n,t} = \mathbb{Q}\big(\sqrt{-3(4nt^3 - 27)}\big)$, as we vary t in $\mathbb{N}_{\geq 3} := \{n \in \mathbb{N} \mid n \geq 3\}$, represents infinitely many imaginary quadratic fields. First, observe there are infinitely many prime divisors of the values of $D(t) := 4nt^3 - 27$ as t varies in $\mathbb{N}_{\geq 3}$ (If $p_1 = 3, p_2, \ldots, p_r$ are the only prime divisors, then we arrive at a contradiction by considering $D(3p_1 \cdots p_r)$.) Now, for any prime $p \geq 5$, if $p \mid D(t)$ for some $t \in \mathbb{N}_{\geq 3}$, then $D(t + p) \equiv D(t) + 12nt^2p \pmod{p^2}$; thus although p divides both $D(t)$ and $D(t + p)$, p^2 can not divide both $D(t)$ and $D(t + p)$, which in-turn implies that infinitely many primes occur in the factorisation of the square-free part of $D(t)$ as t varies in $\mathbb{N}_{\geq 3}$.*

Corollary 4.4. *Let $T(X, Y) \in \mathbb{Z}[X, Y]$ be an irreducible binary cubic such that the discriminant D of $T(X, Y)$ satisfied $D = n^2$ for some $n \in \mathbb{N}$. Then $nT(x, y)$ is a rational cube sum for every $x, y \in \mathbb{Q}$. In particular, every $m \in \{k^2 + k + 7 \mid k \in \mathbb{Z}\}$ is a rational cube sum.*

Proof. Following the proof of Prop. 4.2, in this setting, we can express $3\sqrt{-3D}T(X, Y) = \xi^{+}(X, Y)^3 + \xi^{-}(X, Y)^3$, for some $\xi^{\pm}_{n,t}(X, Y) \in \mathbb{Q}(\sqrt{-3D})[X, Y]$. Now putting $D = n^2$, it is easy to see that for every $x, y \in \mathbb{Q}$, $nf(x, y)$ is a cube sum in $\mathbb{Q}(\zeta_3)$ and hence over $\mathbb{Q}$.

For the second part, for any $k \in \mathbb{Z}$, consider the irreducible cubic polynomial $T_k(X, Y) = X^3 - (k-1)X^2Y - (k+2)XY^2 - Y^3$. Then the discriminant $D(T_k)$ equals $(k^2 + k + 7)^2$. Hence for every $x, y \in \mathbb{Q}$, $(k^2 + k + 7)F_k(x, y)$ is a rational cube sum. In particular, taking $x = 1$ and $y = 0$, we obtain that integers of the form $k^2 + k + 7$ are rational cube sums. □

Remark 4.5. *Let $T(X) \in \mathbb{Z}[X]$ be a monic irreducible cubic polynomial such that $\text{Gal}(T) \cong \mathbb{Z}/3\mathbb{Z}$. Then from Corollary 4.4, it follows that $\sqrt{Disc(T)}$ is rational cube sum. An explicit parametrization of all monic irreducible trinomials $T(X) = X^3 - aX + b$ with $\text{Gal}(T) \cong \mathbb{Z}/3\mathbb{Z}$ can be found in [12, Theorem 4.6].*

Acknowledgments. We are very grateful to Prof. Heath-Brown and Prof. Moroz and for their insightful comments, suggestions and for answering many questions. S. Jha is supported by SERB grant CRG/2022/005923.

Declarations

- Competing interests: Not applicable.

References

[1] Sylvester, J.J.: On certain ternary cubic-form equations. Amer. J. Math. **4**(2), 357–393 (1879)

[2] Selmer, E.: The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. Acta. Math. **85**, 203–362 (1951)

[3] Satgé, P.: Un analogue du calcul de heegner. Invent. Math. **87**(2), 425–439 (1987)

[4] Lieman, D.: Nonvanishing of l-series associated to cubic twists of elliptic curves. Ann. of Math. **140**(1), 81–108 (1994)

[5] Alpöge, L., Bhargava, M., Shnidman, A.: Integers expressible as the sum of two rational cubes, with an appendix by A. Burungale and C. Skinner. preprint, https://arxiv.org/abs/2210.10730

[6] Dasgupta, S., Voight, J.: Heegner points and sylvester's conjecture. In: Arithmetic Geometry, Clay Math. Proc., Amer. Math. Soc, vol. 8 (2009)

[7] Yin, H.: On the case 8 of the sylvester conjecture. Trans. of AMS **375**, 2705–2728 (2022)

[8] Villegas, F.R., Zagier, D.: Which primes are sums of two cubes? In: Number Theory, CMS Conference Proceedings, Amer. Math. Soc., vol. 15, pp. 295–306 (1995)

[9] Heath-Brown, D.R.: Primes represented by $x^3 + 2y^3$. Acta. Math. **186**, 1–84 (2001)

[10] Heath-Brown, D.R., Moroz, B.Z.: Primes represented by binary cubic forms. Proc. London Math. Soc.(3) **84**(2), 257–288 (2002)

[11] Heath-Brown, D.R., Moroz, B.Z.: On the representation of primes by cubic polynomials in two variables. Proc. London Math. Soc. (3) **88**(2), 289–312 (2004)

[12] Majumdar, D., Sury, B.: Cyclic cubic extensions of $\mathbb{Q}$. International J. Number Theory **18**(9), 1929–1955 (2022)

[13] Shu, J., Yin, H.: Cube sums of the forms $3p$ and $3p^2$ ii. Math. Annalen **385**, 1037–1060 (2023)

[14] Jha, S., Majumdar, D., Shingavekar, P.: 3-Selmer group, ideal class groups and cube sum problem. preprint, https://arxiv.org/abs/2207.12487

[15] Majumdar, D., Shingavekar, P.: Cube sum problem for integers having exactly two distinct prime factors. Proceedings - Mathematical Sciences **accepted https://arxiv.org/abs/2211.17118** (2023)

[16] Cai, L., Shu, J., Tian, Y.: Cube sum problem and an explicit gross-zagier formula. Amer. J. Math. **139**(3), 785–816 (2017)

[17] Murty, R., Murty, K.: Mean values of derivatives of modular l-series. Ann. of Math. (2) **133**(3), 447–475 (1991)

[18] Richmond, H.: On analogues of waring's problem for rational numbers. Proc. London Math. Soc. (2) **21**, 401–409 (1923)

[19] Rubin, K.: The "main conjectures" of iwasawa theory for imaginary quadratic fields. Invent. Math. **103**, 25–58 (1991)

[20] Evertse, J.H.: On the representation of integers by binary cubic forms of positive discriminant. Invent. Math. **73**, 117–138 (1983)