Communications in
Number Theory and Physics
Volume 16, Number 2, 401–434, 2022

Diophantine equations with sum of cubes and cube of sum*

Bogdan A. Dobrescu and Patrick J. Fox

We solve Diophantine equations of the type $a\,(x^3+y^3+z^3) = (x+y+z)^3$, where x, y, z are integer variables, and the coefficient $a \neq 0$ is rational. We show that there are infinite families of such equations, including those where a is any cube or certain rational fractions, that have nontrivial solutions. There are also infinite families of equations that do not have any nontrivial solution, including those where $1/a = 1-24/m$ with restrictions on the integer m. The equations can be represented by elliptic curves unless $a = 9$ or 1, and any elliptic curve of nonzero j-invariant and torsion group $\mathbb{Z}/3k\mathbb{Z}$ for $k = 2, 3, 4$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ corresponds to a particular a. We prove that for any a the number of nontrivial solutions is at most 3 or is infinite, and for integer a it is either 0 or ∞. For $a = 9$, we find the general solution, which depends on two integer parameters. These cubic equations are important in particle physics, because they determine the fermion charges under the $U(1)$ gauge group.

AMS 2000 subject classifications: Primary 11D25; secondary 11G05, 11D45, 11D85.
Keywords and phrases: Cubic Diophantine equations, elliptic curves, primitive solutions, fibonacci numbers.

*This work was supported by Fermi Research Alliance, LLC under Contract DE-AC02-07CH11359 with the U.S. Department of Energy.

1. Introduction

The study of elliptic curves provides powerful tools for solving cubic Diophantine equations [1, 2, 3]. Nevertheless, it remains challenging to find general solutions to parametric families of cubic Diophantine equations [4, 5]. Here we study the following family of cubic equations in the integer variables x, y, z:

$$a\left(x^3 + y^3 + z^3\right) = (x + y + z)^3 \quad , \tag{1.1}$$

where the coefficient a is a rational number.

These homogeneous Diophantine equations have applications in particle physics, related to the allowed charges of spin-1/2 particles under a new $U(1)$ gauge group [6, 7, 8, 9]. Since $a = 0$ is a trivial case ($x = -y - z$), we will focus on $a \neq 0$. To characterize the solutions to (1.1), we introduce some definitions.

Definition 1. Two integers, x and y, form a *vectorlike pair* if $x + y = 0$.

This terminology is common in quantum field theory, where x and y are fermion charges, and the gauge field has vector couplings to the fermions if $x + y = 0$.

Definition 2. A *primitive solution* to Eq. (1.1) is a solution $\{x, y, z\}$ with $x, y, z \in \mathbb{Z}$ that satisfies the following conditions:
1. $xyz \neq 0$.

2. $\gcd(x, y, z) = 1$.
3. the set $\{x, y, z\}$ does not include any vectorlike pair.

Note that for $a \neq 1$ the condition $xyz \neq 0$ implies that the set $\{x, y, z\}$ does not include any vectorlike pair. Thus, the third condition is relevant only for $a = 1$.

Definition 3. A *general solution* to the Diophantine equation (1.1) for fixed a is a solution which depends on at most 2 integer parameters such that any primitive solution can be obtained, after removing $\gcd(x, y, z)$ and up to a reordering or an overall sign, for some values of the parameters.

Although we refer to Eq. (1.1) as "cube of sum proportional to the sum of cubes", it is useful to note that the change of variables

$$\begin{aligned} x &= \frac{1}{2}(t - u + v) \quad , \\ y &= \frac{1}{2}(t + u - v) \quad , \\ z &= \frac{1}{2}(-t + u + v) \quad , \end{aligned} \tag{1.2}$$

where $t, u, v \in \mathbb{Z}$, transforms Eq. (1.1) into a cubic equation involving the product of the variables and the cube of their sum:

$$(a - 1)(t + u + v)^3 = 24a\, t\, u\, v \quad . \tag{1.3}$$

This equation has solutions for $a = 1$ only with $tuv = 0$, corresponding to $\{x, y, z\}$ solutions to Eq. (1.1) which include a vectorlike pair. Thus, there are no primitive solutions for $a = 1$.

Eq. (1.1) for $a \neq 0, 1$ is also related to a parametric family of elliptic curves over rational numbers. To see that, let us change variables through

$$\begin{aligned} x &= 3a(3a - X)\,\mathcal{R} \quad , \\ y &= \left(\frac{9}{2}a^2(a - 1) + Y\right)\mathcal{R} \quad , \\ z &= \left(\frac{9}{2}a^2(a - 1) - Y\right)\mathcal{R} \quad , \end{aligned} \tag{1.4}$$

where X, Y are rational variables, and $\mathcal{R} \in \mathbb{Q}$ is an overall normalization

chosen such that $x, y, z \in \mathbb{Z}$. Eq. (1.1) then becomes

$$Y^2 = X^3 - 27a^3X - \frac{27}{4}a^4\left((a-3)^2 - 12\right) \quad . \tag{1.5}$$

The discriminant of this elliptic curve is

$$\Delta = -3^9\, a^8\, (a-1)^3\, (a-9) \quad . \tag{1.6}$$

The only relevant value of a that makes the discriminant vanish is $a = 9$. It turns out that this is also the most interesting case for simple extensions of the Standard Model of particle physics [6].

In Section 2 we show that any equation of the type (1.1) with a given by the ratio of any perfect cubes, or by certain rational fractions, has nontrivial solutions. In Section 3 we prove that there are no primitive solutions for certain infinite families of rational a, and then use properties of the elliptic curves to prove that the number of primitive solutions is at most 3 or is infinite. Section 4 focuses on integer values of a, including all the solutions to Eq. (1.1) in the particular case where two variables are equal. This provides a further restriction on the number of primitive solutions, which for integer a can be 0 or ∞. We also present there a 2-parameter solution for $a = 9$, and prove its generality. Then, we identify solutions for infinite sequences of a equal to a perfect square (*e.g.,* squared Fibonacci numbers of even index), which are relevant for particle physics. In Section 5 we summarize our results.

2. Infinite families of equations with solutions

The existence of primitive solutions to Eq. (1.1) depends on the value of a. In this section we identify a few infinite families of equations with rational values for a that allow primitive solutions.

2.1. Primitive solutions when a is a rational fraction

Theorem 1. *The equation with integer variables* x, y, z

$$p^3\left(x^3 + y^3 + z^3\right) = q^3(x+y+z)^3 \tag{2.1}$$

has at least one primitive solution for any $p, q \in \mathbb{Z}$ *with* $q/p \neq 0, 1, -1/2$.

Proof. Let us express the variables as cubic polynomials in p and q as follows:

$$x = (p+2q)\left(p^2 + pq + 4q^2\right) \quad ,$$

$$y = -3q\left(p^2 + 2pq + 3q^2\right) \quad , \tag{2.2}$$
$$z = -p^3 - 3p^2q - 6pq^2 + q^3 \quad .$$

It can be checked that the above expressions represent a solution to Eq. (2.1) for any p, q. The necessary conditions $x \neq 0$ and $y \neq 0$ imply $p \neq -2q$ and $q \neq 0$, while $z \neq 0$ is satisfied for any rational p/q. To identify the primitive solutions, it remains to impose that no two variables form a vectorlike pair, *i.e.*,

$$x + y = p^3 - q^3 \neq 0 \quad , \tag{2.3}$$
$$y + z = -(p + 2q)^3 \neq 0 \quad ,$$
$$z + x = 9q^3 \neq 0 \quad ,$$

so that $p \neq q$. If $\gcd(x, y, z) \neq 1$, then $\{x, y, z\}$ is not a primitive solution. In that case, a primitive solution is $\{x, y, z\}/\gcd(x, y, z)$ with x, y, z given in (2.2). □

Remark. The solution constructed in (2.2) is not generically unique. For example, $p = 2$, $q = 1$, (*i.e.*, $a = 8$) leads to $\{x, y, z\} = \{40, -33, -31\}$, but the simpler solution $\{5, 4, 3\}$ is not included in (2.2).

Proposition 2. *Equation* (1.1) *has at least one primitive solution iff* a *is of the form*

$$a = \frac{(s+2)^3}{6r^2 + s^3 + 2} \tag{2.4}$$

for any $r, s \in \mathbb{Q}$ *satisfying* $s \neq 0$, $|r| \neq 1$ *and* $r \neq \pm(s+1)$.

Proof. Put $r = r_1/r_2$, $s = s_1/s_2$, with $r_1, r_2, s_1, s_2 \in \mathbb{Z}$, $r_2 s_2, \neq 0$ $\gcd(r_1, r_2) = \gcd(s_1, s_2) = 1$. The triple $\{x, y, z\} = \{s_1 r_2\,, s_2(r_2 + r_1)\,, s_2(r_2 - r_1)\}$ is a solution to Eq. (1.1) for a given by (2.4). This is not a vectorlike solution (see Definition 2) iff $r \neq \pm(s+1)$. The $xyz \neq 0$ condition is satisfied for any $r \neq \pm 1$, $s \neq 0$. Note that $\gcd(x, y, z) = 2^\delta \gcd(s_2, r_2)$, where $\delta = 1$ if s_1 is even and $r_1 r_2$ is odd, and $\delta = 0$ otherwise. Thus,

$$\frac{\{\, s_1 r_2\ ,\ s_2(r_2 + r_1)\ ,\ s_2(r_2 - r_1)\,\}}{2^\delta \gcd(s_2, r_2)} \tag{2.5}$$

is a primitive solution. To prove the converse, for any primitive solution $\{x, y, z\}$, the value of a extracted from Eq. (1.1) is identical to (2.4) with

$$r = \frac{x-y}{x+y} \quad , \quad s = \frac{2z}{x+y} \quad . \tag{2.6}$$

Since $xyz(x+y)(y+z) \neq 0$, the values $r = \pm 1$, $s = 0$, and $r = \pm(s+1)$ are not allowed. Given that $(6r^2 + s^3 + 2)(x+y)^3 = x^3 + y^3 + z^3$, Fermat's Last Theorem (FLT) for exponent 3 ensures that the denominator of (2.4) is nonzero. □

Remark. For $s = 1$ and $r = p/q$ with $p, q \in \mathbb{Z}$ coprime, (2.4) gives the infinite family of a values

$$a = \frac{9q^2}{2p^2 + q^2} \quad , \tag{2.7}$$

which have primitive solutions iff $q \neq 0$ and $\pm p/q \neq 1, 2$: $\{x, y, z\} = \{p + q\,,\, q\,,\, -p + q\}$. Within this family, there are only three integer values of a that allow primitive solutions: $p = 1$, $q = 2$ gives $a = 6$ and the solution $\{3, 2, 1\}$; $p = 1$, $q = 4$ gives $a = 8$ and $\{5, 4, 3\}$; $p = 0$, $q = 1$ gives $a = 9$ and $\{1, 1, 1\}$.

An infinite family with the coefficient a given by the reciprocal of an integer is obtained from Proposition 2 by setting $r = p/q$, $s = -2 + 1/q$, with $q \notin \{0, \pm p, 1 \pm p\}$. The ensuing family of equations, spanned by the two integers p, q, is

$$x^3 + y^3 + z^3 = \left[6q\left(p^2 - (q-1)^2\right) + 1\right](x + y + z)^3 \quad , \tag{2.8}$$

and has the primitive solution $\{1 - 2q,\, p + q,\, -p + q\}$.

Many other simple families may be obtained from Proposition 2. For example, $s = -1$ gives $1/a = 6r^2 + 1$, $s = -3$ gives $1/a = 25 - 6r^2$, and $s = 2$ gives $a = 32/(3r^2 + 5)$. Some infinite families of integer a with primitive solutions are derived in Section 4.1. Despite the versatility of (2.4), the methods employed in this subsection are not helpful for proving Theorem 1 because it is nontrivial to find the solutions (2.2).

2.2. General solution for two variables

In this subsection we seek all the solutions to Eq. (1.1) that have one of the variables equal to zero. It is sufficient to consider the Diophantine equation

in two variables:

$$a\left(x^3+y^3\right)=(x+y)^3 \quad , \tag{2.9}$$

where $a \in \mathbb{Q}$. Trivial (vectorlike) solutions with $y=-x$ exist for any a. If $xy=0$, then solutions with a single nonzero variable exist only for $a=1$. Leaving aside these trivial cases, the following Proposition provides the full solution to the equation with "cube of sum proportional to the sum of cubes" in two variables. As we seek nontrivial solutions, we remove an $x+y$ factor, so that Eq. (2.9) is equivalent to (2.10) given below.

Proposition 3. *The equation with integer variables* x, y

$$(a-1)(x^2+y^2)=(a+2)\,x\,y \quad , \tag{2.10}$$

where $a \in \mathbb{Q}$*, has solutions with* $xy(x+y) \neq 0$ *iff* a *is of the form*

$$a=\frac{4}{1+3\,\alpha^2} \quad , \tag{2.11}$$

where α *is any rational number except* ± 1*.*

Proof. If a is given by (2.11), then it is straightforward to check that any integers x, $y \neq 0$ that satisfy

$$\frac{x}{y}=\frac{\alpha \pm 1}{1 \mp \alpha} \quad \text{for} \quad \forall\, \alpha \neq 0, \pm 1\,, \quad \text{or} \quad x=y \quad \text{for} \quad \alpha=0 \tag{2.12}$$

provide a solution to (2.10).

To prove the reverse, we note that if $\{x, y\}$ is a solution to (2.10) with $x+y \neq 0$, then the equation can be written as

$$\frac{4}{a}=1+3\left(\frac{x-y}{x+y}\right)^2 \quad , \tag{2.13}$$

so that a is given by (2.11) with

$$\alpha=\pm\frac{x-y}{x+y} \quad . \tag{2.14}$$

□

The first part of Proposition 3 proves in particular that there is an infinite family of rational values for a, given in (2.11), for which (1.1) has solutions

with $xy(x+y) \neq 0$ and $z = 0$. The following corollary shows that the situation is different when $a \in \mathbb{Z}$.

Corollary 4. *Up to a reordering or an overall integer rescaling, there are only two solutions to Eq. (2.9) with $xy(x+y) \neq 0$ when the coefficient a is an integer: $x = 2$, $y = 1$ for $a = 3$, and $x = y = 1$ for $a = 4$.*

Proof. Eq. (2.11) implies $0 < a \leq 4$. From Eq. (2.10) follows that for $a = 1$ there are no solutions with $xy(x+y) \neq 0$. Also, there are no solutions for $a = 2$ because in that case there is no rational value of α that satisfies (2.11). For $a = 3$, $x/y = 2$ or $1/2$, while $a = 4$ gives $x = y$.

Corollary 5. *The general solution $\{x, y\}$ to Eq. (2.9) with $xy(x+y) \neq 0$, up to an overall rescaling by an integer and an $x \leftrightarrow y$ interchange, is $\{x, y\} = \{p+q\,,\, p-q\}$, where $p, q \in \mathbb{Z}$ such that $\alpha = q/p \neq \pm 1$ in (2.11).*

Proof. Solving (2.14) for x/y gives (2.12) or the same with x and y interchanged. Replacing $\alpha = q/p$ in (2.14) gives $x = p + q$, $y = p - q$ up to an overall normalization.

Some numerical examples with noninteger a, are $p = 2$, $q = 3$, which gives $a = 12/7$ and the solution $\{5, 1\}$, and $p = 1$, $q = 2$, which gives $a = 16/7$ and the solution $\{3, 1\}$.

3. The number of primitive solutions

For certain values of a it is possible to prove that there exist no primitive solutions to Eq. (1.1). We invoke the results of E. Dofs [11, 12] to show that there are infinite families of rational a (including certain integer values) for which there are no solutions. We then use of elliptic curves to determine the number of primitive solutions for fixed a.

3.1. Infinite families of equations with no primitive solution

Using the change of variables presented in (1.2), the "cube of sum proportional to the sum of cubes" equation can be related to a homogenous cubic equation, shown in (1.3), where the cube of a sum of 3 integers is proportional to their product. This allows us to invoke existing results to show that there is a set of rational a for which there are no solutions, including the integer values $a = -23, -5, -3, -2, 4, 7, 25$.

Theorem 6. *There are no primitive solutions to Eq. (1.1) if*

$$a = \frac{p^n}{p^n - 24} \tag{3.1}$$

for $a \neq -1/11$, $p \equiv 2 \bmod 3$ *prime,* $n \geq 1$ *integer with* $3 \nmid n$, *and all prime factors of* $p^n - 27$ *congruent to* $2 \bmod 3$.

Proof. For $a \in \mathbb{Q}$ satisfying (3.1), use the change of variables (1.2) to rewrite (1.1) in the form

$$(t + u + v)^3 = p^n \, t \, u \, v \quad . \tag{3.2}$$

The variables t, u, v are pairwise coprime, which implies that any solution must take the form $t = t_0^3$, $u = u_0^3$, $v = p^k v_0^3$, with $k = 1$ or 2, $n = 3n' - k$, $p \nmid t_0, u_0$, and the integer variables t_0, u_0, v_0 are pairwise coprime. Thus, (3.2) becomes

$$t_0^3 + u_0^3 + p^k v_0^3 = p^{n'} t_0 u_0 v_0 \ . \tag{3.3}$$

We now use a theorem of Dofs [11], which investigates solutions to equations of the form $p^{\omega_1} t_0^3 + p^{\omega_2} u_0^3 + p^{\omega_3} v_0^3 = d \, t_0 u_0 v_0$. Dofs defines a quantity $F = d^3 - 27 p^{\omega_1 + \omega_2 + \omega_3}$, and determines the solvability of the above equation when all prime factors of F are $2 \bmod 3$ and certain conditions on F, p, and d are satisfied.

For Eq. (3.3) these conditions determine that if $k = 1$ (case N_{01} in Dofs' proof) there are no nontrivial solutions unless $p = 2$ and $n' = 2$ (*i.e.* $a = 4$). In that case the only solution is $t_0 = u_0 = v_0 = 1$, corresponding to $\{x, y, z\} = \{1, 0, 1\}$, which is not a primitive solution to (1.1). If $k = 2$ (case N_{02} in Dofs' proof) there are no nontrivial solutions unless $p = 2$ and $n' = 1$ (*i.e.* $a = -1/11$) when the only solution is $\{t_0, u_0, v_0\} = \{1, 1, -1\}$, which corresponds to the primitive solution $\{x, y, z\} = \{-2, 3, -2\}$. □

Remark. The values $a = -23, -2, 4, 25$ are the only integer ones that yield $24a/(a-1)$ as a non-cubic power of a single prime: 23, 2^4, 2^5, 5^2, respectively. Thus, $a = -23$, which corresponds to $n = n' = 1$, $k = 2$, and $a = -2$ ($n' = k = 2$) can be seen to have no solution. For $a = 4$ ($n' = 2, k = 1, p = 2$) there is a solitary solution to (3.3) which is not a primitive solution to (1.1). The case of $a = 25$ corresponds to $p = 5, k = 1, n' = 1$ and has no solution (see also [13]).

Theorem 7. *There are no primitive solutions to Eq. (1.1) for*

$$a = \frac{p\,q^2}{p\,q^2 - 24} \ , \tag{3.4}$$

with $(p,q) \in \{(2,3),(5,2),(7,2)\} \cup \{(2,Q)|\ Q \equiv 1 \bmod 3$ *prime,* $2Q^2 - 27$ *prime, and* 4 *is a cubic non-residue* $\bmod Q\}$.

Proof. Consider the rational coefficient a of the more general form

$$a = \frac{p^n q^m}{p^n q^m - 24} \ , \tag{3.5}$$

where $p \neq q$, $n = 3n' - k_p$ and $m = 3m' - k_q$ with $k_p, k_q = 1$ or 2. Changing variables from $\{x,y,z\}$ to $\{t,u,v\}$ as in (1.2), Eq. (1.1) becomes

$$\left(\frac{t+u+v}{p^{n'}q^{m'}}\right)^3 = \frac{t\,u\,v}{p^{k_p}\,q^{k_q}} \ . \tag{3.6}$$

The fact that t,u,v are pairwise coprime implies that at least one variable is a perfect cube. Without loss of generality, we take $t = t_0^3$. For the other variables, up to a reordering, there are two cases:

$$u = u_0^3 \ , \ v = p^{k_p}q^{k_q}v_0^3 \qquad \text{or} \qquad u = p^{k_p}u_0^3 \ , \ v = q^{k_q}v_0^3 \ . \tag{3.7}$$

The first case is similar to the one encountered in the derivation of Eq. (3.3), and implies

$$t_0^3 + u_0^3 + p^{k_p}q^{k_q}v_0^3 = p^{n'}q^{m'}t_0u_0v_0 \ . \tag{3.8}$$

In the second case, defining new variables

$$\begin{aligned} T &= t^2u + u^2v + v^2t - 3\,t\,u\,v \\ U &= t\,u^2 + u\,v^2 + v\,t^2 - 3\,t\,u\,v \\ V &= \frac{1}{p^{n'}q^{m'}}\left(t^3 + u^3 + v^3 - 3\,t\,u\,v\right) \end{aligned} \tag{3.9}$$

transforms Eq. (3.2) into a cubic Diophantine equation of the same form as (3.8),

$$T^3 + U^3 + p^{k_p}q^{k_q}V^3 = p^{n'}q^{m'}TUV \ . \tag{3.10}$$

Thus, if this equation has no solution, neither will (1.1) with a given by (3.5). Dofs [12] has carried out an investigation of the conditions under which (3.10) is unsolvable for $k_q = 1$ and $k_p \leq 3$. Restricting further to $n = 1, m = 2$ leads to the result of use here. We refer the reader to [12] for details but point out that $(p, q) = (2, 3)$ satisfies the unsolvability conditions of case (ii, c) of Dofs [12], while all other values for (p, q) listed after (3.4) satisfy case (i) of Dofs and so can be determined to have no solution. □

The first three values for (p, q) targeted by Theorem 7 lead to integer a: $-3, -5$, and 7, respectively. The remaining values form a family of rational a for which there are no solutions:

$$a = \left(1 - \frac{12}{Q^2}\right)^{-1} \quad , \tag{3.11}$$

where Q satisfies the conditions of Theorem 7. The following Proposition addresses the structure of the prime numbers Q that define this family.

Proposition 8. *For any $Q \equiv 1 \, mod \, 3$ prime, a necessary condition for 4 to be a cubic non-residue* mod Q *is that*

$$Q = \frac{1}{4}\left(L^2 + 27M^2\right) \tag{3.12}$$

with L and M odd.

Proof. By definition, 4 is a cubic non-residue mod Q if there exists no integer s with $s^3 \equiv 4 \bmod Q$. A necessary condition is that 2 is a cubic non-residue mod Q. It can be shown [14] that any $Q \equiv 1 \bmod 3$ prime can be written as (3.12) with $L, M > 0$ uniquely determined integers. Furthermore, 2 is a cubic residue mod Q iff L and M are even [15]. Thus, 2 is a cubic non-residue mod Q iff both L and M are odd. □

The first four values of Q that satisfy the conditions of Theorem 7 are $Q = 7, 13, 37, 67$, and the corresponding values of (L, M) are (1,1), (5,1), (11,1), (5,3). The ensuing values of a, for which there are no primitive solutions to Eq. (1.1), are 49/37, 169/157, 1369/1357, 4489/4477.

3.2. Testing for primitive solutions with elliptic curves

Using the transformation of (1.4), the "cube of sum proportional to the sum of cubes" equation can be converted to an elliptic curve (E), given in (1.5), allowing one to bring to bear all of the powerful machinery associated with

their study [1, 2, 3]. The Mordell-Weil theorem [16] states that the set of rational points on an elliptic curve, $E(\mathbb{Q})$, form a finitely generated Abelian group and as such can be separated into sets of points of finite order, the torsion group(s), and the set of points of infinite order. The number of infinite order points is the rank of the Mordell-Weil group of $E(\mathbb{Q})$. Thus, if the rank is 0, then the number of rational points on E is finite, and the points are generated by the members of the torsion group.

The rank and the generators of the torsion group can be efficiently calculated, for any given value of a, by computer algebra systems such as `PARI/GP` [17]. Some of the algorithms rely on the Birch and Swinnerton-Dyer conjecture [18], which relates the rank of $E(\mathbb{Q})$ to the order of the zero of a certain L-function, $L(E, s)$, at $s = 1$, the so-called analytic rank. The conjecture has been proved [19] for curves whose rank is 0 or 1, and thus this procedure is adequate for our purpose of determining the number of solutions to Eq. (1.1) for given a.

The elliptic curve (1.5) is in the Weierstrass reduced form,

$$Y^2 = X^3 + AX + B \quad , \tag{3.13}$$

with $A = -27a^3$, $B = -(27/4)a^4\left(a^2 - 6a - 3\right)$. The j-invariant of this curve is

$$j_a = -\frac{(24A)^3}{\Delta} = -\frac{2^{12}\,3^3\,a}{(a-1)^3\,(a-9)} \quad , \tag{3.14}$$

where we used the discriminant $\Delta = -16\left(4A^3 + 27B^2\right)$ computed in (1.6). Birational transformations, $X \to r_b^2 X$, $Y \to r_b^3 Y$ with $r_b \in \mathbb{Q}$, and more complicated isogenies do not change the j-invariant.

For the curve (3.13) with $\Delta \neq 0$ and integer A, B, the Nagell-Lutz theorem [20] ensures that any rational point that belongs to the torsion group has integer coordinates. Thus, when the A, B coefficients are noninteger, it is useful to perform a birational transformation that gives integers coefficients. For any $a = a_L/a_R$, with $a_L, a_R \in \mathbb{Z}$, the elliptic curve (1.5) can be transformed into an elliptic curve with integer coefficients:

$$Y_0^2 = X_0^3 - 432\,a_L^3 a_R X_0 - 432\,a_L^4\left(a_L^2 - 6a_L a_R - 3a_R^2\right) \quad , \tag{3.15}$$

where the new variables are $X_0 = (2a_R)^2 X$, $Y_0 = (2a_R)^3\,Y$. The corresponding solution to (1.1), up to an overall normalization similar to that shown in

(1.4), is given by

$$\begin{aligned} x &= 6a_L\,(12a_La_R - X_0) \quad , \\ y, z &= 36\,a_L^2\,(a_L - a_R) \pm Y_0 \quad . \end{aligned} \tag{3.16}$$

Note that the points $\pm P_V$ on the elliptic curve (3.15) of integer coordinates $12a_L^2\,\big(1, \pm 3(a_L - a_R)\big)$ correspond to the vectorlike solutions $x + y = z = 0$ and $x + z = y = 0$. Furthermore, d^2Y_0/dX_0^2 vanishes at $\pm P_V$, so these two inflection points and the point at infinity (labelled $\mathcal{O}_\infty$) form a $\mathbb{Z}_3$ subgroup of the torsion group. This implies that the torsion group, which in general can be any of the 15 discrete groups listed in [21], is constrained in our case to be one of only 5 groups: $\mathbb{Z}_{3n}$ with $1 \leq n \leq 4$, and $\mathbb{Z}_2 \times \mathbb{Z}_6$ (we use the short-hand notation $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$). In Section 4 we will show that this list is significantly shorter when $a \in \mathbb{Z}$. Examples of elliptic curves of various torsion groups and ranks can be found at [22]. These can be transformed into the Weierstrass reduced form and compared with (3.15) up to a birational transformation, checking if they are consistent with integer values for a_L and a_R. We next prove some results about the number and properties of primitive solutions to (1.1).

Proposition 9. *For any set of non-vectorlike integer solutions to Eq. (1.1) with $a \in \mathbb{Q}$, $a \neq 0, 1, 9$, obtained by a reordering or an overall rescaling of $\{x, y, z\}$, there exist 6 rational points on the elliptic curve (1.5) when x, y, z do not include two equal variables, or 3 rational points when two variables are equal.*

Proof. If $\{x, y, z\}$ is a non-vectorlike solution to Eq. (1.1) with $a \neq 0, 1$, then from (1.4) follows that (X_1, Y_1) are two rational points on the elliptic curve (1.5) with

$$(X_1, \pm Y_1) = \left(3a - \frac{x}{3a\mathcal{R}_1} \;\;, \pm\frac{y - z}{2\mathcal{R}_1}\right) \quad , \quad \mathcal{R}_1 = \frac{y + z}{9a^2(a - 1)} \quad . \tag{3.17}$$

Given that $\{y, z, x\}$ and $\{z, x, y\}$ are also solutions, there are two more pairs of rational points, $(X_i, \pm Y_i)$ with $i = 2, 3$, whose coordinates are given by the appropriate permutations of x, y, z in (3.17). Thus, generically, for all the solutions obtained by a reordering or an overall rescaling of $\{x, y, z\}$, there are 6 rational points whose coordinates are given by (3.17) and its permutations. It is straightforward to check that the 6 rational points are distinct when no two of the x, y, z variables are equal.

If two of the x, y, z variables are equal, then two of the pairs of rational points are identical, and the third pair has $Y_i = 0$, so only 3 rational points

are distinct. The case with $x = y = z$ is not relevant here, as it occurs only for the singular curve with $a = 9$. □

Theorem 10. *The torsion group of the elliptic curve (1.5) is* $\mathbb{Z}_9$ *iff the rational coefficient* a *in Eq. (1.1) satisfies*

$$a^{-1} = 1 - 3\left(\frac{2f(f-1)}{f^3 - 3f^2 + 1}\right)^3 \quad , \tag{3.18}$$

where $f \in \mathbb{Q}$, $f \neq 0, 1$.

Proof. Following Kubert's parametrization [23], the elliptic curve in rational variables X_K, Y_K can be written as

$$Y_K^2 + (1 - c_K) Y_K X_K - b_K Y_K = X_K^2 \left(X_K - b_K\right) \quad , \tag{3.19}$$

where $b_K, c_K \in \mathbb{Q}$, $b_K \neq 0$. The point $P_0 = (0, 0)$ is of maximal finite order. Following the method of Reichert [24], we repeatedly use the group addition on P_0: $2P_0 = (b_K\,,\, b_K c_K)$, $3P_0 = (c_K\,,\, b_K - c_K)$. For $c_K \neq 0$ and $b_K \neq c_K$ we also obtain

$$\begin{aligned} 4P_0 &= \frac{b_K}{c_K^2}\left(b_K - c_K\ ,\ b_K(c_K + 1) - \frac{b_K^2}{c_K}\right) \quad , \\ 5P_0 &= \frac{b_K\, c_K^2}{(b_K - c_K)^2}\left(c_K + 1 - \frac{b_K}{c_K}\ ,\ b_K - \frac{c_K^3}{b_K - c_K}\right) \quad . \end{aligned} \tag{3.20}$$

The above signs in $Y_K(4P_0)$ differ from those in [24], and agree with [25].

The torsion group of the elliptic curve is $\mathbb{Z}_9$ iff $X_K(5P_0) = X_K(4P_0)$, which requires

$$c_K^2 + c_K - b_K = \left(\frac{b_K}{c_K} - 1\right)^3 \quad . \tag{3.21}$$

Imposing that the left-hand term is a cube, chosen for convenience to be $(2f - 1)^3$ with $f \in \mathbb{Q}$, gives

$$b_K = c_K\left(f^2 - f + 1\right) \quad , \quad c_K = f^2\left(f - 1\right) \quad . \tag{3.22}$$

This agrees with [23], and differs slightly from [26]. The conditions $b_K c_K \neq 0$ and $b_K \neq c_K$ are satisfied for any $f \neq 0, 1$.

The elliptic curve (3.19) can be transformed to the reduced Weierstrass form by putting

$$\begin{aligned} X_K &= r_b^2 X + \frac{b_K - c_\star^2}{3} \quad , \\ Y_K &= r_b^3 Y - c_\star r_b^2 X - \frac{c_\star}{3}\left(b_K - c_\star^2\right) + \frac{b_K}{2} \quad , \end{aligned} \tag{3.23}$$

where $c_\star = (1-c_K)/2$, and r_b is the parameter of a birational transformation. The Weierstrass coefficients A_K and B_K are polynomials in b_K, c_K, divided by r_b^4 and r_b^6, respectively. The requirement that the discriminant of (3.19) is nonzero gives the condition

$$D_K = 2b_K^2 - b_K\left(4c_\star^2 - 9c_\star + 27/8\right) + 2c_\star^4 - c_\star^3 \neq 0 \quad . \tag{3.24}$$

The j-invariant of (3.19) and also of the transformed curve is

$$j_K = \frac{2^9}{D_K}\left(b_K - 2c_\star^2 + 3c_\star + c_\star^4/b_K\right)^3 \quad . \tag{3.25}$$

In the case of the $\mathbb{Z}_9$ torsion group, the restriction (3.22) ensures that (3.24) is satisfied, and it implies that A_K, B_K become polynomials of order 12, respectively 18, in f, labelled by A_f and B_f. A necessary condition for our elliptic curve (3.15) to have the $\mathbb{Z}_9$ torsion group is that its points of order 3, given by $(X, Y) = 3a^2(1, \pm 3(a-1)/2)$, are identified with the points $3P_0$ or $-3P_0$ on $Y^2 = X^3 + A_f X + B_f$, which have coordinates

$$X(3P_0) = \frac{1}{12\, r_b^2}\left(f^3 - 3f^2 + 1\right)^2 \quad , \quad Y(\pm 3P_0) = \mp\frac{f^3}{2\, r_b^3}\,(f-1)^3 \quad . \tag{3.26}$$

This identification implies that a must satisfy (3.18), or the analogous relation with a sign flip in front of the parenthesis. The j-invariant obtained by inserting the restriction (3.22) in (3.25) can then be compared with (3.14), and the $j_K = j_a$ identity is obtained only for the sign assignment in (3.18). Furthermore, no rational value for f allows the equality of the j-invariants for the other sign assignment. Thus, (3.18) is also a sufficient condition for the $\mathbb{Z}_9$ torsion group. □

Proposition 11. *Any elliptic curve with torsion group $\mathbb{Z}_6$ and nonzero j-invariant, or with torsion group $\mathbb{Z}_9$, $\mathbb{Z}_{12}$, or $\mathbb{Z}_2 \times \mathbb{Z}_6$, is equivalent to Eq. (1.1) for a particular $a \in \mathbb{Q}$.*

Proof. Equating the j-invariants j_K, given in (3.25), and j_a, given in (3.14), leads to a quartic equation for a in terms of b_K, c_K. When the torsion group is $\mathbb{Z}_6$, $\mathbb{Z}_9$, $\mathbb{Z}_{12}$ or $\mathbb{Z}_2 \times \mathbb{Z}_6$ the parametrization for b_K, c_K given by Kubert [23] leads to a rational root of the quartic. The general parametrization for an elliptic curve with torsion group $\mathbb{Z}_6$ or $\mathbb{Z}_2 \times \mathbb{Z}_6$ is given by (3.19) with $b_K = c_K + c_K^2$ for $c_K \neq 0, -1, -1/9$, and the rational solution for a satisfies

$$a^{-1} = 1 - 24\,\frac{c_K^2(c_K+1)}{(3c_K+1)^3} \quad . \tag{3.27}$$

The $j_K = 0$ curve with $\mathbb{Z}_6$ torsion has $c_K = -1/3$, and cannot be obtained from (1.5) for any a. Any Kubert curve (3.19) with $\mathbb{Z}_6$ torsion and $j_K \neq 0$ can be transformed into our elliptic curve (1.5) using (3.23) with

$$r_b = \frac{3c_K\left(3 + c_K + c_K^2\right) + 1}{6\,(3c_K+1)^2} \quad . \tag{3.28}$$

For torsion group $\mathbb{Z}_2 \times \mathbb{Z}_6$, the same forms for a and r_b as in (3.27) and (3.28) are valid with the restriction $c_K = 2(5-\alpha)/(\alpha^2-9)$, where $\alpha \in \mathbb{Q}$ and $\alpha \neq 1, \pm 3, 5, 9$.

For torsion group $\mathbb{Z}_{12}$ the general parameterization [23] has b_K, c_K as rational fractions of a parameter $\tau \in \mathbb{Q}$, $\tau \neq 0, 1, 1/2$, and the rational solution of the quartic satisfies

$$a^{-1} = 1 - 24\,\frac{\sigma^4(4\sigma+1)(2\sigma+1)}{\Big(6\sigma(\sigma+1)+1\Big)^3} \quad , \tag{3.29}$$

with $\sigma = \tau(\tau-1)$. In this case, the r_b parameter in transformation (3.23) is given by τ^3 times a rational fraction in σ. The solution for torsion group $\mathbb{Z}_9$ is given in (3.18). □

Proposition 12. *The number n_a of primitive solutions to Eq. (1.1), up to a reordering of the variables or an overall sign change, satisfies $0 \leq n_a \leq 3$ or is infinite.*

Proof. For each rational point (X, Y) on the elliptic curve (1.5) corresponding to an $\{x, y, z\}$ solution to Eq. (1.1), Proposition 9 ensures that there are only five or two other rational points that correspond to the same solution up to a reordering of x, y, z. If the rank of the elliptic curve is $r(E) \geq 1$, then the number of rational points is infinite, and thus the number of $\{x, y, z\}$ solutions with $\gcd(x, y, z) = 1$ is infinite. Up to a reordering or a sign change,

there is a single vectorlike solution with $\gcd(x, y, z) = 1$, and at most one non-vectorlike solution (see Corollary 5) with $xyz = 0$ for any given $a \neq 1$, the number of primitive solutions is $n_a = \infty$ when $r \geq 1$. Examples of rank 1 include $a = -1, 3, 6$. If the discriminant Δ given in (1.6) is 0, then $a = 1$ and $n_a = 0$, or $a = 0, 9$ which gives $n_a = \infty$ (the case $a = 9$ is solved in Theorem 18).

It remains to consider the case where $r(E) = 0$. In that case, the number of rational points is finite, and is given by the number of elements of the torsion group that are different from $\mathcal{O}_\infty$. As there are exactly two rational points corresponding to vectorlike solutions, namely $(X, Y) = 3a^2(1, \pm 3a(a-1)/2)$, the number of rational points that may correspond to primitive solutions is 0 for $\mathbb{Z}_3$, 3 for $\mathbb{Z}_6$, 6 for $\mathbb{Z}_9$, and 9 for $\mathbb{Z}_{12}$ or $\mathbb{Z}_2 \times \mathbb{Z}_6$. Thus, if the torsion group is $\mathbb{Z}_3$ and $r(E) = 0$, then $n_a = 0$. As an example, for $a = 16$ the elliptic curve after the birational transformation $X = 4\tilde{X}$, $Y = 8\tilde{Y}$ becomes $\tilde{Y}^2 = \tilde{X}^3 - 432\tilde{X} - 16956$. Using `PARI/GP`, we find $r(E) = 0$ and the torsion group $\mathbb{Z}_3$ generated by $(\tilde{X}, \tilde{Y}) = (48, \pm 270)$, corresponding to the vectorlike solution $\{1, -1, 0\}$.

Proposition 9 implies that for $\mathbb{Z}_6$ there is a single primitive solution when $a \neq 4$, and that solution has two equal variables. An example is $a = -1/11$, and the primitive solution is $\{3, -2, -2\}$. For $a = 4$, the torsion group is $\mathbb{Z}_6$ but $n_a = 0$ because $xyz = 0$, as shown in the proof to Theorem 6. From Proposition 9 follows that $n_a = 1$ also occurs for any a (as determined by Theorem 10) that gives the $\mathbb{Z}_9$ torsion group, but there are no two equal variables in this case. For example, $a = 9/73$ gives the primitive solution $\{7, -5, 1\}$. The $\mathbb{Z}_{12}$ group gives $n_a = 2$, and a single primitive solution has two equal variables. For $a = -1331/8389$, the primitive solutions are $\{29, -20, -20\}$, $\{43, -41, -13\}$. The $\mathbb{Z}_2 \times \mathbb{Z}_6$ group gives $n_a = 3$, and each solution has two equal variables. This is possible only for $\Delta > 0$, *i.e.*, $1 < a < 9$. For example, $a = 343/127$ gives the primitive solutions $\{5, 1, 1\}$, $\{4, 4, -1\}$, $\{11, -9, -9\}$. Thus, there are values of $a \in \mathbb{Q}$ for each of the $n_a = 0, 1, 2, 3, \infty$ cases. The existence of the vectorlike solutions and the Mazur theorem [21] ensure that (1.5) cannot have other torsion groups. □

4. Integer a

Let us restrict the analysis to $a \in \mathbb{Z}$. We first identify an infinite family of a values that allow primitive solutions. We then find that only for $a = 9$ are there primitive solutions with two equal variables. We also present the general solution for $a = 9$, which involves two parameters. This is followed by a proof that the number of primitive solutions for any integer a is either infinite or 0.

4.1. Infinite families of solutions for integer a

Proposition 13. *For each equation (1.1) with*

$$a = (-1)^n F_n^2 \quad , \tag{4.1}$$

where F_n is the Fibonacci number of integer $n \geq 1$, $n \neq 2$, there is at least one primitive solution with $x > -y > -z > 0$.

Proof. Using (2.4) for $s = -4/3$ and $r = p/(9q)$, where $p, q \in \mathbb{Z}$ and $q \neq 0$, gives the infinite family of a values

$$a = \frac{4q^2}{p^2 - 5q^2} \quad . \tag{4.2}$$

Proposition 2 ensures that Eq. (1.1) has at least one primitive solution for each of the a values in (4.2) iff $\pm p/q \neq 3, 9$. From (2.5) follows that a primitive solution is given by

$$\{x, y, z\} = \frac{\{\, 12q \;,\; -p-9q \;,\; p-9q \,\}}{2^\delta \, \gcd(p, 3) \, \gcd(p, q)} \quad , \tag{4.3}$$

where $\delta = 1$ if pq is odd, and $\delta = 0$ otherwise. An infinite subset of the family of equations (4.2) is obtained for $p = L_n$ and $q = F_n$, where L_n and F_n are the Lucas and Fibonacci numbers with $n \geq 1$ ($n = 2$ is not allowed because it gives $p/q = 3$). The identity $L_n^2 = 5F_n^2 + 4(-1)^n$ implies that a is, up to a sign, the square of the nth Fibonacci number, as in (4.1). To determine the solution arising from (4.3) for each n, we use the identities $L_n = F_n + 2F_{n-1}$ and $\gcd(F_m, F_n) = F_{\gcd(m,n)}$ (see page 190 of [4]), which imply $2^\delta \gcd(L_n, F_n) = 2$. Furthermore, $3|L_n$ iff $n \equiv 2 \bmod 4$, so the primitive solution becomes

$$\{x, y, z\} = \frac{1}{3^\theta}\{\, 6F_n \;,\; -5F_n - F_{n-1} \;,\; -4F_n + F_{n-1} \,\} \quad , \tag{4.4}$$

where $\theta = 1$ for $n \equiv 2 \bmod 4$, and $\theta = 0$ otherwise. This solution to (1.1) satisfies $x > -y > -z > 0$ for any $n \geq 1$. □

In particular, $n = 1$ gives $a = -1$ and the solution $\{6, -5, -4\}$, while $n = 3$ gives $a = -4$ and the solution $\{12, -11, -7\}$. The case of n even gives an infinite family of equations with a as a perfect square, discussed further in Section 4.5. Other families of solutions defined by recurrence relations can be obtained from the results of [10] for an equation related to (1.3).

Remark. For $r = -6q^3$, $s = -6q^2$, with $q \in \mathbb{Z}_{\neq 0}$, Proposition 2 yields the infinite family of negative integers $a = -4(3q^2 - 1)^3$ with the primitive solutions $\{-6q^2, 1 - 6q^3, 1 + 6q^3\}$. For $a = p^3$, Theorem 1 ensures at least one primitive solution for each $p \in \mathbb{Z}$, $p \neq 1, -2$.

4.2. Solutions with $y = z$

We now show that the Diophantine equation (1.1) has solutions with two equal variables, when a is integer, only for $a = 9$ if $xyz \neq 0$. In the case where one variable is zero, Corollary 4 implies that the other two variables are equal and nonzero only for $a = 4$.

Before proving the main result of this section (Theorem 15), it is useful to solve the following Thue equation with integer variables:

$$x^3 + 2y^3 = 2 \quad . \tag{4.5}$$

This belongs to a family of equations shown by Delaunay and Nagell (see [27, 28]) to have at most one solution with $xy \neq 0$. We prove a stronger statement, using classical methods (the same result can be obtained using a computer algebra system, such as `PARI/GP`).

Lemma 14. *The Diophantine equation (4.5) has no solution with $x \neq 0$.*

Proof. If $3|y$, then $x \equiv 2 \bmod 3$, implying $x^3 \equiv -1 \bmod 9$, in contradiction to $9|y^3$. If $y \equiv 2 \bmod 3$, then $x^3 \equiv 4 \bmod 9$, which is impossible for a cube. For $y \equiv 1 \bmod 3$, Eq. (4.5) uniquely splits into two parts proportional to perfect cubes:

$$2(1 - y) = 9f^3 \quad , \tag{4.6}$$

$$(y + 2)^3 - (y - 1)^3 = (3g)^3 \quad , \tag{4.7}$$

where $f, g \in \mathbb{Z}$, $f, g \neq 0$, $\gcd(f, g) = 1$, and $x = 3fg$. Eq. (4.7) is in contradiction to FLT unless $y = 1$ or $y = -2$. These values are not allowed by $x \neq 0$ and Eq. (4.6). □

Theorem 15. *If there exists a primitive solution $\{x, y, z\}$ to Eq. (1.1) with $a \in \mathbb{Z}$, $a \neq 9$ and $a \neq 0$, then no two variables can be equal. For $a = 9$, there are only two primitive solutions with $y = z > 0$: $x = y = 1$ and $x = -5$, $y = 4$.*

Proof. For $y = z$, Eq. (1.1), takes the form

$$a\left(x^3 + 2y^3\right) = (x + 2y)^3 \quad . \tag{4.8}$$

For $|a| \geq 2$, let $p \geq 2$ be a prime divisor of a, and $n_p \geq 1$ be the multiplicity of p in the prime factorization of a. Eq. (4.8) requires $x \equiv -2y \mod p$, which together with $\gcd(x, y) = 1$ implies $p \nmid y$. If $3 \nmid n_p$, then Eq. (4.8) also requires $x^3 \equiv -2y^3 \mod p$, which gives $p|(6y^3)$. Hence, $p = 2$ or $p = 3$, so that a is of the form $a = 2^{n_2}3^{n_3}b^3$, with $n_2, n_3, b \in \mathbb{Z}$, $n_2, n_3 \geq 0$, $b \neq 0$, $2 \nmid b$ and $3 \nmid b$. Eq. (4.8) then splits into two equations:

$$x + 2y = b\,c \quad , \tag{4.9}$$

$$2^{n_2}3^{n_3}(x^3 + 2y^3) = c^3 \quad , \tag{4.10}$$

where $c \in \mathbb{Z}_{\neq 0}$. Any solution $\{x, y\}$ for $c < 0$ implies the solution $\{-x, -y\}$ for $c \to -c$, so it is sufficient to consider $c > 0$. The first equation requires $\gcd(c, y) = \gcd(b, y) = 1$. Eliminating x from (4.9) gives

$$2^{n_2+1}3^{n_3+1}y(b\,c - y)^2 = \left(2^{n_2}3^{n_3}\,b^3 - 1\right)c^3 \quad . \tag{4.11}$$

Since $\gcd(c, y(bc - y)) = 1$, c cannot have prime divisors other than 2 or 3. Given that the parenthesis on the right-hand side of (4.11) is not divisible by 2 unless $n_2 = 0$, and not divisible by 3 unless $n_3 = 0$, the above equation can be satisfied only in four cases:

Case 1) $n_2 = n_3 = 0$, $c = 1$. Eq. (4.10) becomes $x^3 + 2y^3 = 1$, which has no solution with $y \neq 0$ other than $y = -x = 1$ (see [28] or page 34 of [3]). Thus, (4.9) implies $b = 1$, so that $a = 1$, and Eq. (4.8) has no primitive solution.

Case 2) $n_2 \equiv 2 \mod 3$, $n_3 = 0$, $c = 2^{(n_2+1)/3}$. Eq. (4.10) is given by $x^3 + 2y^3 = 2$, which following Lemma 14 has no solution with $x \neq 0$.

Case 3) $n_2 = 0$, $n_3 \equiv 2 \mod 3$, $c = 3^{(n_3+1)/3}$. Eqs. (4.9)-(4.10) are now $x+2y = 3^{(n_3+1)/3}\,b$ and $x^3+2y^3 = 3$. The only solutions to the latter equation are $x = y = 1$ and $x = -5$, $y = 4$ [27, 28]. Both solutions correspond to $n_3 = 2$ and $b = 1$, so $a = 9$.

Case 4) $n_2 \equiv 2 \mod 3$, $n_3 \equiv 2 \mod 3$, $c = 2^{(n_2+1)/3}3^{(n_3+1)/3}$. Eq. (4.10) becomes $x^3 + 2y^3 = 6$, and Nagell's theorem [27, 28] allows at most one solution. A solution exists, namely $x = 2$, $y = -1$, but in this case (4.9) gives $b = 0$, so this is not a solution with $a \neq 0$. □

4.3. General solution for $a = 9$

Focusing on Eq. (1.1) with $a = 9$,

$$9\,(x^3 + y^3 + z^3) = (x + y + z)^3 \quad , \tag{4.12}$$

we present a 2-parameter solution, and prove that it is the general solution. There exist trivial (vectorlike) solutions to (4.12) of the type $x = -y$, $z = 0$, and obvious permutations. All other solutions have $xyz \neq 0$ and are primitive up to a rescaling. Among these, Theorem 15 identifies $\{1, 1, 1\}$ and $\{5, -4, -4\}$, which up to an overall sign or a reordering are the only primitive solutions to Eq. (1.1), for any a, with two equal variables.

Lemma 16. *All integer solutions* $\{x, y, z\}$ *of Eq.* (4.12) *with* $\gcd(x, y, z) = 1$, *other than* $x = y = z = \pm 1$, *are given by*

$$\{x, y, z\} = \{\,(\ell_1 + \ell_2)\left(\ell_1^2 + \ell_2^2 + \frac{\ell_1\ell_2}{2}\right)\,,\ \ell_2^3 - x\,,\ \ell_1^3 - x\,\}\quad , \tag{4.13}$$

where the integer parameters ℓ_1, ℓ_2 *are coprime.*

Proof. Changing variables through the inverse of the transformation (1.2), which is

$$t = x + y \quad , \quad u = y + z \quad , \quad v = z + x \quad , \tag{4.14}$$

we find that Eq. (4.12) becomes

$$\left(\frac{t + u + v}{3}\right)^3 = t\,u\,v \quad . \tag{4.15}$$

For primitive solutions, $xyz \neq 0$ so that $tuv \neq 0$, and $\gcd(x, y, z) = 1$ requires t, u, v to be pairwise coprime, unless $|xyz| = 1$ in which case $t = u = v = \pm 2$. We ignore the case of $x = y = z = \pm 1$ from now on. Since (4.15) implies that tuv is a perfect cube, each of t, u, v must be a perfect cube. Without loss of generality, take $t = \ell_2^3$ and $v = \ell_1^3$ with $\gcd(\ell_1, \ell_2) = 1$, which gives y and z in (4.13). Setting $u = u_0^3$, (4.15) becomes

$$(u_0 + \ell_1 + \ell_2)\left(u_0^2 - (\ell_1 + \ell_2)u_0 + \ell_1^2 - \ell_1\ell_2 + \ell_2^2\right) = 0 \quad . \tag{4.16}$$

The solution $u_0 = -\ell_1 - \ell_2$ gives the expression for x in (4.13). There is no other integer solution, because the second factor in (4.16) is quadratic

in u_0 and has discriminant $-3(\ell_1 - \ell_2)^2$. Note that the solution with zero discriminant, which is $t = u = v = \pm 1$, does not correspond to $x, y, z \in \mathbb{Z}$.

For vectorlike solutions $xyz = t\,u\,v = 0$. Any vectorlike solution with $\gcd(x, y, z) = 1$ is obtained from (4.13) when $\ell_1 = \pm 1, \ell_2 = 0$, or $\ell_1 = 0, \ell_2 = \pm 1$, or $\ell_1 = -\ell_2 = \pm 1$. □

Corollary 17. *For any primitive solution to Eq.* (4.12) *other than* $\{1, 1, 1\}$, *the sum of any two variables is a perfect cube.*

Proof. Theorem 16 implies that

$$\begin{aligned} t &= x + y = \ell_2^3 \ , \\ u &= y + z = -(\ell_1 + \ell_2)^3 \ , \\ v &= z + x = \ell_1^3 \ , \end{aligned} \tag{4.17}$$

where $\ell_1, \ell_2 \in \mathbb{Z}$. □

Remark. Using transformation (1.4) for $a = 9$, we see that Eq. (4.12) becomes a singular curve in X and Y. Setting $X = 3^4(\tilde{X} - 1)$, $Y = 3^6\tilde{Y}$, the singular curve takes the form

$$\tilde{Y}^2 = \tilde{X}^2\left(\tilde{X} - 3\right) \ . \tag{4.18}$$

All rational solutions to this equation other than $\tilde{X} = \tilde{Y} = 0$ (which corresponds to $x = y = z$) are given by $\tilde{X} = \mu^2 + 3$, $\tilde{Y} = \mu(\mu^2 + 3)$, with $\mu \in \mathbb{Q}$. After removing a common factor of -3^6, this corresponds to the solution

$$\{x, y, z\} = \{\, 3\mu^2 + 5 \ , \ -\left(\mu^3 + 3\mu + 4\right) \ , \ -y - 8 \,\} \ . \tag{4.19}$$

If μ is noninteger, this is a rational solution that can be turned into an integer one by an overall rescaling. Taking $\mu = (\ell_1 - \ell_2)\,/\,(\ell_1 + \ell_2)$, and removing an overall factor of 8, reproduces the solution (4.13). This provides an alternative proof to Lemma 16. Note that the vectorlike solution $y + z = 0$ (which corresponds to $\ell_1 = -\ell_2$) cannot be recovered for any finite μ. However, the ordering of x, y, z in (4.19) is arbitrary, and changing it would allow the $y + z = 0$ solution. The fact that not all vectorlike solutions can be obtained for the same ordering is true for any a, as can be seen in transformation (1.4).

Theorem 18. *The general solution to Eq.* (4.12) *is given by*

$$x = \frac{1}{2}\left(\ell_1^3 + \ell_2^3 + (\ell_1 + \ell_2)^3\right) + \delta_{\ell_1,0}\,\delta_{\ell_2,0} \ ,$$

$$y = \frac{1}{2}\left(-\ell_1^3 + \ell_2^3 - (\ell_1+\ell_2)^3\right) + \delta_{\ell_1,0}\,\delta_{\ell_2,0} \quad , \tag{4.20}$$

$$z = \frac{1}{2}\left(\ell_1^3 - \ell_2^3 - (\ell_1+\ell_2)^3\right) + \delta_{\ell_1,0}\,\delta_{\ell_2,0} \quad ,$$

with the two integer parameters satisfying $\ell_1 \geq \ell_2 \geq 1$ *and* ℓ_1, ℓ_2 *coprime, or* $\ell_1 = \ell_2 = 0$. *Each solution is generated by a unique* ℓ_1, ℓ_2 *pair.*

Proof. Following Definition 3, we need to show that any primitive solution to Eq. (4.12) is obtained for some values of ℓ_1, ℓ_2, up to a variable reordering or an overall sign change. For $\ell_1 = \ell_2 = 0$, (4.20) gives the primitive solution $\{1, 1, 1\}$. For any $\ell_1 \neq 0$ and $\ell_2 \neq 0$, it is straightforward to check that (4.20) represents a solution with $xyz \neq 0$, which means that it is a primitive solution (see Definition 2).

Theorem 16 ensures that any primitive solution other than $\{1, 1, 1\}$ is obtained for certain values of ℓ_1 and ℓ_2. Primitive solutions have $\gcd(x, y, z) = 1$, and thus can be obtained only for $\gcd(\ell_1, \ell_2) = 1$. The reverse is also true, because $\gcd(x, y, z) = \gcd(x + y, y + z, z + x) = \gcd(\ell_1, \ell_2)$.

The interchange of ℓ_1 and ℓ_2 leads only to the interchange of x and y, and thus the same primitive solution up to a reordering. Likewise, a sign flip of both ℓ_1 and ℓ_2 only flips the sign of the whole set $\{x, y, z\}$. Hence, it is sufficient to take $\ell_1 \geq |\ell_2|$.

Solution (4.20) is also invariant under

$$\begin{aligned} \ell_2\,, \ell_1 \quad &\to \quad -\ell_2\,,\ \ell_1 + \ell_2 \quad , \\ x\,, y \quad &\to \quad -y\,, -x \quad , \end{aligned} \tag{4.21}$$

so it is sufficient to take $\ell_2 \geq 1$. It remains to show that no primitive solution can be obtained for two different values of the ℓ_1, ℓ_2 pair. To see that, note that the solution (4.20) satisfies (4.17). Furthermore, for $\ell_1 \geq \ell_2 \geq 1$ all the solutions satisfy $x \geq |y| \geq |z| \geq 1$, so a different ℓ_1, ℓ_2 pair cannot lead to the same solution with a different ordering of the variables. Hence, for each primitive solution $\{x, y, z\}$ there is a unique choice of ℓ_1, ℓ_2 (the simplest examples are collected in Table 1). □

A solution to (4.12) in terms of three integer parameters is given in [8]; since the number of parameters is equal to the number of variables, that does not represent a general solution (see Definition 3). A solution to (4.15) in terms of a rational parameter given in [29] can be shown to be equivalent to (4.17), but the generality of the solution is not investigated there.

4.4. Properties of primitive solutions

Theorem 19. *For any fixed $a \in \mathbb{Z}$, the number of primitive solutions to Eq. (1.1) is either 0 or ∞.*

Proof. From Theorem 18 follows that the number n_a of primitive solutions to Eq. (1.1) for $a = 9$ is infinite. As $n_a = 0$ for $a = 1$, and $n_a = \infty$ for $a = 0$, it is sufficient to consider integer a values for which the discriminant (1.6) is nonzero. As shown in the proof to Proposition 12, n_a is finite and nonzero iff the elliptic curve (1.5) has rank 0 and the torsion group given by one of the following four possibilities: $\mathbb{Z}_6$, $\mathbb{Z}_9$, $\mathbb{Z}_{12}$ or $\mathbb{Z}_2 \times \mathbb{Z}_6$. With the exception of $\mathbb{Z}_9$, all these torsion groups imply that at least one primitive solution has two equal variables. The latter condition is forbidden by Theorem 15 when $a \in \mathbb{Z}$.

It thus remains to show that the torsion group cannot be $\mathbb{Z}_9$ for integer a. Theorem 10 establishes that if $\mathbb{Z}_9$ is the torsion group of (1.5), then

$$a = \frac{q^3}{q^3 - 3\,p^3} \quad , \tag{4.22}$$

where $p, q \in \mathbb{Z}$ are coprime, $pq \neq 0$, and

$$\frac{p}{q} = \frac{2f(f-1)}{f^3 - 3f^2 + 1} \tag{4.23}$$

with $f \in \mathbb{Q}$, $f \neq 0, 1$. As a is an integer, it follows that $(q^3 - 3p^3)|q^3$, and $\gcd(p, q) = 1$ implies that $q^3 - 3p^3 = 1$, or $q = 3q_0$ and $9q_0^3 - p^3 = 1$ for

Table 1: All primitive solutions to equation (4.12) with $x \leq 200$ generated by the general solution (4.20), and the corresponding ℓ_1, ℓ_2 parameters

Primitive solution ($a = 9$)	$\ell_1\,,\ell_2$
$\{1, 1, 1\}$	$0\,,0$
$\{5, -4, -4\}$	$1\,,1$
$\{18, -17, -10\}$	$2\,,1$
$\{46, -45, -19\}$	$3\,,1$
$\{80, -72, -53\}$	$3\,,2$
$\{95, -94, -31\}$	$4\,,1$
$\{171, -170, -46\}$	$5\,,1$

Table 2: Number n_a of primitive solutions to (1.1) for $a \in \mathbb{Z}$, $|a| \leq 10$

a	n_a	Proof	Low-lying primitive solutions
1	0	See (1.3)	
-1	∞	rank 1, Proposition 12	$\{6,-5,-4\}$, $\{1670,-1661,-339\}$
2	0	rank 0, Theorem 19	
-2	0	Theorem 6	
3	∞	rank 1, Proposition 12	$\{10,-9,-7\}$, $\{190,153,-28\}$
-3	0	Theorem 7	
4	0	Theorem 6	
-4	∞	rank 1, Proposition 12	$\{12,-11,-7\}$, $\{23807,-22655,-11640\}$
5	0	rank 0, Theorem 19	
-5	0	Theorem 7	
6	∞	rank 1, Proposition 12	$\{3,2,1\}$, $\{20,-17,-15\}$
-6	0	rank 0, Theorem 19	
7	0	Theorem 7	
-7	0	rank 0, Theorem 19	
8	∞	rank 1, Proposition 12	$\{5,4,3\}$, $\{40,-33,-31\}$
-8	0	rank 0, Theorem 19	
9	∞	General solution (4.20)	Table 1
-9	0	rank 0, Theorem 19	
± 10	0	rank 0, Theorem 19	

$q_0 \in \mathbb{Z}$. The first of these two cubic Thue equations has no solution with $pq \neq 0$. The $9q_0^3 - p^3 = 1$ equation with $q_0 \neq 0$ has only the solution $p = 2$, $q_0 = q/3 = 1$, which is not consistent with the constraint (4.23) for any rational f. □

Theorem 19 implies that for any integer $a \neq 0, 1, 9$ the torsion group is $\mathbb{Z}_3$, and its elements are the vectorlike solutions. Furthermore, there are no primitive solutions iff the elliptic curve (1.5) has rank 0, which can be checked using computer algebra systems. Theorem 19 also implies that when primitive solutions exist for integer a, their number is infinite. In Table 2 we show results for all integer $a \neq 0$ with $|a| \leq 10$, indicating either a direct proof, or the rank of (1.5) computed with `PARI/GP`. In all the cases other than $a = 9$ shown in Table 2 where there are primitive solutions (only two of the low-lying ones are displayed), the rank is 1.

Proposition 20. *If $\{x_i, y_i, z_i\}$, $i = 1, 2$, are two different primitive solutions to Eq. (1.1) for any fixed $a \in \mathbb{Q}$, then a third solution is*

(4.24)
$$\{x_3, y_3, z_3\} = \left\{ 3\left(1 - a\, w^2\right) - \bar{x}_1 - \bar{x}_2 \ ,\ \bar{y}_2 + w\left(x_3 - \bar{x}_2\right) \ ,\ a - 1 - y_3 \right\} \ ,$$

where

$$(\bar{x}_i \ , \ \bar{y}_i) = \frac{a-1}{y_i + z_i}\,(x_i \ , \ y_i) \quad , \qquad w = \frac{\bar{y}_2 - \bar{y}_1}{\bar{x}_2 - \bar{x}_1} \quad . \tag{4.25}$$

The $\{x_3, y_3, z_3\}$ solution is not vectorlike iff the two solutions $\{x_i, y_i, z_i\}$, $i = 1, 2$, do not become identical upon an $x_2 \leftrightarrow y_2$ or $x_2 \leftrightarrow z_2$ transposition and possibly an overall sign change. If $\{x_3, y_3, z_3\}\mathcal{R}$ with $\mathcal{R} \in \mathbb{Q}$ is primitive, then $\{x_3, y_3, z_3\}\mathcal{R} \neq \{x_i, y_i, z_i\}$ iff $x_3 \neq \bar{x}_i$.

Proof. The existence of the primitive solutions $\{x_i, y_i, z_i\}$, $i = 1, 2$, implies $a \neq 1$ and $y_i + z_i \neq 0$. As the solutions are different, $\bar{x}_1 \neq \bar{x}_2$, so that the quantities introduced in (4.25) do not have singularities.

Let us define the function $\zeta(x, y, z) = a(x^3 + y^3 + z^3) - (x + y + z)^3$. We find

$$\zeta(x_3, y_3, z_3) = \frac{a-1}{\left(\bar{x}_2 - \bar{x}_1\right)^3}\left(P(\bar{x}_1, \bar{x}_2, \bar{y}_1, \bar{y}_2) - P(\bar{x}_2, \bar{x}_1, \bar{y}_2, \bar{y}_1)\right) \quad . \tag{4.26}$$

The polynomial $P(\bar{x}_1, \bar{x}_2, \bar{y}_1, \bar{y}_2)$ is of degree 6, and is given by

$$P(\bar{x}_1, \bar{x}_2, \bar{y}_1, \bar{y}_2) = \bar{x}_1^6 - 6\bar{x}_1^5 - 3\bar{x}_1^4\left(\bar{x}_2^2 - 2\bar{x}_2 + a - 4\right) + \bar{x}_1^3\, C(\bar{x}_2, \bar{y}_1, \bar{y}_2), \tag{4.27}$$

where $C(\bar{x}_2, \bar{y}_1, \bar{y}_2)$ is a quadratic polynomial in $\bar{x}_2, \bar{y}_1, \bar{y}_2$ with coefficients dependent only on a. Since $\zeta(x_i, y_i, z_i) = 0$ for $i = 1, 2$, we obtain the identities

$$\bar{x}_i^3 = 3\bar{x}_i\left(\bar{x}_i + a - 1\right) - 3a\bar{y}_i\left(\bar{y}_i - a + 1\right) - (a-1)^3 \ , \quad i = 1, 2 \quad . \tag{4.28}$$

We use repeatedly the above identity for $i = 1$ to eliminate all the powers of $\bar{x}_1$ higher than 2 in $P(\bar{x}_1, \bar{x}_2, \bar{y}_1, \bar{y}_2)$. As a result, $\zeta(x_3, y_3, z_3)$ is proportional to $\zeta(x_2, y_2, z_2)$, which proves that $\{x_3, y_3, z_3\}$ is a solution to Eq. (1.1).

The set of two equations $x_3/x_i = y_3/y_i = z_3/z_i$ is solvable iff $x_3 = \bar{x}_i$, for $i = 1, 2$. Given that the rational rescaling $\mathcal{R}$ is chosen such that $\gcd(x_3\mathcal{R}, y_3\mathcal{R}, z_3\mathcal{R}) = 1$, and also $\gcd(x_i, y_i, z_i) = 1$, it follows that $x_3 \neq \bar{x}_i$ is the necessary and sufficient condition for $\{x_3, y_3, z_3\}\mathcal{R} \neq \pm\{x_i, y_i, z_i\}$.

It remains to determine in which cases is the new solution vectorlike. The y_3, z_3 variables cannot form a vectorlike pair because $y_3 + z_3 = a - 1 \neq 0$. Before analyzing the other two pairs, note that $w \neq 0$ because $y_1 \neq y_2$.

If $x_3 + y_3 = 0$, then Eq. (1.1) gives $z_3 = 0$ because $a \neq 1$. From (4.24) then follows that $y_3 = a - 1$, and thus $x_3 = 1 - a$, which in turn leads to two constraints. The first one is $w = -z_2/(x_2 + y_2 + z_2)$, which is equivalent to

$$\frac{z_2}{z_1} = \frac{x_2 + y_2}{x_1 + y_1} \quad . \tag{4.29}$$

The second constraint is that the expression for x_3 in (4.24) equals $1 - a$, and can be written as

$$3\,a\,(\bar{y}_2 - a + 1)^2 = (a + 2 - \bar{x}_1 - \bar{x}_2)\,(\bar{x}_2 + 1)^2 \quad . \tag{4.30}$$

After eliminating x_1 from (4.29) and inserting it in the second constraint, we find

$$\frac{y_1}{z_1} = \frac{x_2}{z_2} + \frac{z_2(-x_2 + y_2 + 2z_2)\,\zeta(x_2, y_2, z_2)}{3az_2(x_2 + y_2)(y_2 + z_2)^2 - z_2\,\zeta(x_2, y_2, z_2)} \quad . \tag{4.31}$$

Since $\zeta(x_2, y_2, z_2) = 0$, we obtain $y_1/z_1 = x_2/z_2$, and using again (4.29) the result is that $x_3 + y_3 = 0$ iff $x_2/y_1 = y_2/x_1 = z_2/z_1$. Taking into account that $\gcd(x_i, y_i, z_i) = 1$, the latter condition is equivalent to $x_2 = y_1$ and $y_2 = x_1$.

Analogously, $x_3 + z_3 = 0$ iff $x_2 = z_1$ and $z_2 = x_1$. This means that $\{x_3, y_3, z_3\}$ is not vectorlike unless the two initial primitive solutions become identical (possibly up to an overall sign) after one transposition. □

It is straightforward to extend Proposition 20 to include non-vectorlike solutions that have one variable equal to 0, as given in Corollary 5. Note also that Proposition 20 does not preclude that $\{x_3, y_3, z_3\}\mathcal{R}$ equals to $\pm\{x_i, y_i, z_i\}$ after a reordering of x_i, y_i, z_i. The next corollary takes advantage of the fact that a primitive solution is different than the one obtained by any reordering, when no two variables are equal.

Corollary 21. *If $\{x_1, y_1, z_1\}$ is a primitive solution to Eq. (1.1) for $a \in \mathbb{Z}$, then a non-vectorlike solution is*

$$\{x, y, z\} = \left\{ 3\,\frac{1 - aw^2}{a - 1} - \frac{x_1}{y_1 + z_1} - \frac{y_1}{z_1 + x_1} \;,\; wx + \frac{z_1 - w\,y_1}{z_1 + x_1} \;,\; 1 - y \right\} , \tag{4.32}$$

where

$$w = \frac{x_1\, y_1 - z_1^2}{(x_1 - y_1)\,(x_1 + y_1 + z_1)} \quad . \tag{4.33}$$

For $xyz \neq 0$, this solution becomes primitive upon a rational rescaling, and is different from $\{x_1, y_1, z_1\}$ iff $x \neq x_1/(y_1 + z_1)$.

Proof. Replacing $\{x_2, y_2, z_2\}$ by $\{y_1, z_1, x_1\}$ in (4.24) and (4.25), and removing an overall factor of $a - 1$, we obtain (4.32), so Proposition 20 guarantees that $\{x, y, z\}$ is a solution. For integer a, Theorem 15 ensures that the variables x_1, y_1, z_1 are all different, so that $\{x_1, y_1, z_1\}$ differs from $\{y_1, z_1, x_1\}$ by two transpositions. Proposition 20 then implies that $\{x, y, z\}$ is not vectorlike. Thus, for $xyz \neq 0$ (which is guaranteed by Corollary 4 for $a \neq 3$), there exists $\mathcal{R} \in \mathbb{Q}$ such that $\{x, y, z\}\mathcal{R}$ is primitive. From Proposition 20 also follows that $\{x, y, z\}\mathcal{R} \neq \{x_1, y_1, z_1\}$ iff $x \neq x_1/(y_1 + z_1)$. □

The fact that two primitive solutions can be combined to produce a third one, as shown in Proposition 20, is related to the group law for addition of rational points on elliptic curves. Likewise, the use of a single primitive solution to construct a new one, as in (4.32), is related to the group addition of a rational point to itself. For any integer a, Theorem 4.4 ensures that if a primitive solution exists, then the number of primitive solutions is infinite. Using a single primitive solution $\{x_1, y_1, z_1\}$ to produce (4.32), then reordering the new solution and using it together with $\{x_1, y_1, z_1\}$ to produce a third one, and repeating the last step indefinitely would generate an infinite set of primitive solutions. For example, take $a = -1$ and the solution $\{6, -5, -4\}$. The constructed solution (4.32), after a rational rescaling is $\{1661, -1670, 339\}$. Applying (4.24) to $\{6, -5, -4\}$ and $\{1661, 339, -1670\}$ gives the primitive solution $\{-16490494, 17520795, -8126864\}$, and so on.

4.5. Coefficient a as a perfect square – applications to physics

We now turn to Diophantine equations of the type (1.1) in the special case where $a \in \mathbb{Z}$ is a perfect square. Putting $a = N^2$, we seek primitive solutions to

$$N^2 \left(x^3 + y^3 + z^3\right) = (x + y + z)^3 \quad , \tag{4.34}$$

where $N \in \mathbb{Z}$, $N \geq 1$. For $N = 1, 2, 4, 5$ there are no primitive solutions, as proved in Sections 1 and 3. For $N = 3$, the general solution to (4.34) is given in (4.20).

An infinite family of equations, where a is a perfect square, that allow primitive solutions is given by $a = k^6$ with $k \in \mathbb{Z}$, $k \neq 0, \pm 1$. In that case, (2.2) implies that a primitive solution to (4.34) with $N = k^3$ is

$$\begin{aligned} x &= \left(k^2+2\right)\left(k^4+k^2+4\right) \quad , \\ y &= -3\left(k^4+2k^2+3\right) \quad , \\ z &= -k^6-3k^4-6k^2+1 \quad . \end{aligned} \tag{4.35}$$

In particular, $N = 8$ gives the solution $\{16, -9, -15\}$, after the gcd is removed.

Another infinite family is given by the Fibonacci numbers of even index,

$$N = F_{2k} \quad , \tag{4.36}$$

with $k \geq 2$, as follows from Proposition 13. The solution

$$x = 6F_{2k} \ , \ y = -5F_{2k} - F_{2k-1} \ , \ z = -4F_{2k} + F_{2k-1} \tag{4.37}$$

is primitive if k is even, or becomes primitive after dividing by $\gcd(x, y, z) = 3$ if k is odd. For $k = 2$, we obtain $N = 3$ and the third solution of Table 1. For $k = 3$, $N = 8$ and the obtained solution is the same as that from the cubic family above. For $k = 4$, $N = 21$, and (4.37) gives the solution $\{126, -118, -71\}$.

Eq. (4.34) is important for particle physics [6, 7, 8]: x, y, z are the charges of three right-handed neutrinos under a new $U(1)$ gauge group, and N is the number of generations of standard fermions, whose $U(1)$ charges are assumed to be generation independent. Eq. (4.34) represents the only nontrivial combination of anomaly equations for a gauge group given by the direct product of the Standard Model $SU(3) \times SU(2) \times U(1)$ group and the new $U(1)$ group, in the presence of three fermions which are singlets under the Standard Model group.

Within the Standard Model, particle physics experiments have established that the number of fermion generations is $N = 3$, so that the general solution (4.20) for $a = 9$ is particularly relevant. Nevertheless, additional hidden sector particles may have another $SU(3) \times SU(2) \times U(1)$ gauge group, and a different number of fermion generations, so that the results for an arbitrary integer $N \geq 1$ are still relevant for particle physics.

To understand why Eq. (4.34) must be satisfied by the $U(1)$ charges of three right-handed neutrinos, one needs to solve first the anomaly equations that arise from triangle diagrams involving two Standard Model gauge bosons

and one $U(1)$ bosons. This fixes the $U(1)$ charges of all standard fermions in terms of two quark charges, labelled z_q and z_u [6]. The remaining anomaly equations include one due to a diagram with two gravitons and one $U(1)$ boson,

$$N\,(z_u - 4z_q) = x + y + z \quad , \tag{4.38}$$

and one due to a diagram with three $U(1)$ bosons,

$$N\,(z_u - 4z_q)^3 = x^3 + y^3 + z^3 \quad . \tag{4.39}$$

Eliminating $z_u - 4z_q$ from these equations gives Eq. (4.34). The primitive solutions are the important ones for particle physics, as they represent the allowed charges for a set of chiral (*i.e.*, non-vectorlike) fermions, which are the only fermions that are likely to be light enough to be within experimental reach.

The family of solutions (4.36) shows that there are anomaly-free gauge charge assignments when the number of generations is given by any Fibonacci number of even index. Combining with the $N = k^3$ family of solutions, the number of fermion generations may belong to the infinite sequence: 3, 8, 21, 27, 55, 64, 125, 144, ... There are, however, many values for N different than k^3 or F_{2k}. A numerical search utilizing `PARI/GP` [17] shows that the number of fermion generations may belong to the sequence (truncated at $N \leq 150$):

$$\begin{aligned} N \in \{&3, 8, 10, 17\text{–}23, 25, 27\text{–}29, 32, 34\text{–}39, 42, 43, 47, 50\text{–}53, 55, 56, \\ &60, 61, 64\text{–}66, 69\text{–}77, 79, 81, 83, 85, 86, 89, 92\text{–}95, 97, 99, 105, \\ &107, 109, 111\text{–}119, 122\text{–}125, 127, 129, 130, 133\text{–}135, 137, 138, \\ &141\text{–}145, 147, 148, \dots\} \quad , \end{aligned} \tag{4.40}$$

where the dash between two numbers indicates that all the integers in that range are included in the sequence. Theorem 19 implies that the number of primitive solutions to Eq. (4.34) is infinite for each value of N in the above sequence.

5. Conclusions

We have solved Diophantine equations of the class "cube of sum proportional to the sum of cubes" (1.1), for various infinite families of rational a (see Section 2). We have proved that for other infinite families of rational a there exist no primitive solutions (see Section 3.1). The properties of elliptic curves

allow the use of numerical methods to decide the solvability for any fixed a (see Section 3.2). Furthermore, the structure of the torsion group determines the number n_a of primitive solutions. When the rank of the elliptic curve is 0, n_a can be at most 3 and there are five possible torsion groups, while for integer a there are no primitive solutions and the torsion group is $\mathbb{Z}_3$ (Theorem 19). Thus, when any primitive solutions exist for some integer a (see, *e.g.*, Table 2), their number is infinite. When a primitive solution is known, other ones can be constructed using the method presented in Corollary 21. We have also shown that any elliptic curve with torsion group $\mathbb{Z}_6$ (for nonzero j-invariant), $\mathbb{Z}_9$, $\mathbb{Z}_{12}$, or $\mathbb{Z}_2 \times \mathbb{Z}_6$, is a particular case of Eq. (1.1).

The case where a is the square of an integer is important for questions that arise in particle physics. The anomaly equations for certain $U(1)$ gauge extensions of the Standard Model of particle physics lead to Eq. (1.1), where the variables are gauge charges of new fermions, and the $U(1)$ charges of the quarks and leptons are generation independent. In particular, $a = 9$ corresponds to three generations of fermions, as in the Standard Model, with one right-handed neutrino per generation. For $a = 9$ we have presented a solution, (4.20), where the variables x, y, z are given by homogeneous cubic polynomials in two integer parameters, and then we have proven that this is the general solution. More generally, if $a = N^2$, then there are solutions when N is given by any Fibonacci number of even index, by any perfect cube (see Section 4.5), or by other integers belonging to the sequence shown in (4.41). Seeking an analytic understanding of that sequence remains a challenge.

References

[1] J. H. Silverman, "The Arithmetic of Elliptic Curves," 2nd edition, Springer, 2009. MR2514094

[2] J. E. Cremona, "Algorithms for Modular Elliptic Curves", 2nd edition, Cambridge Univ. Press, 1997, homepages.warwick.ac.uk/staff/J.E.Cremona/book/fulltext

[3] N. P. Smart, "The Algorithmic Resolution of Diophantine Equations," Cambridge Univ. Press, 1998. MR1689189

[4] G. H. Hardy and E. M. Wright, "An introduction to the theory of numbers", Oxford Univ. Press, 6th edition, 2008. MR2445243

[5] L. E. Dickson, "History of the Theory of Number", Vol. 2, Dover Publications, 2005. L. J. Mordell, "Diophantine Equations", Academic Press, 1969. MR0249355

[6] T. Appelquist, B. A. Dobrescu and A. R. Hopper, "Nonexotic neutral gauge bosons," Phys. Rev. D **68**, 035012 (2003) [hep-ph/0212073].

[7] Y. Cui and F. D'Eramo, "Surprises from complete vector portal theories: New insights into the dark sector and its interplay with Higgs physics," Phys. Rev. D **96**, no. 9, 095006 (2017) [arXiv:1705.03897].

[8] B. C. Allanach, B. Gripaios and J. Tooby-Smith, "Solving local anomaly equations in gauge-rank extensions of the Standard Model," Phys. Rev. D **101**, 075015 (2020) [arXiv:1912.10022]. MR4100339

[9] D. B. Costa, B. A. Dobrescu and P. J. Fox, "General solution to the U(1) anomaly equations," Phys. Rev. Lett. **123**, 151601 (2019) [arXiv:1905.13729]; "Chiral Abelian gauge theories with few fermions," Phys. Rev. D **101**, 095032 (2020) [arXiv:2001.11991].
B. C. Allanach, B. Gripaios and J. Tooby-Smith, "Geometric general solution to the $U(1)$ anomaly equations," JHEP **05**, 065 (2020) [arXiv:1912.04804]. MR4023590

[10] S. A. Brueggeman, "Integers representable by $(x+y+z)^3/xyz$," Int. J. Math. & Math. Sci. 21, 107 (1998). MR1486965

[11] E. Dofs, "On some classes of homogeneous ternary cubic diophantine equations", Ark. Mat. **13** (1975), 29–72, projecteuclid.org/euclid.afm/1485896418

[12] E. Dofs, "Unsolvable Cases of $P^3+Q^3+cR^3 = dPQR$", Rocky Mountain Journal of Mathematics, **28** (1998), 927–938, projecteuclid.org/euclid.rmjm/1181071746

[13] M. Ward, "The vanishing of the homogeneous product sum of the roots of a cubic", Duke Math. J. **26** (1959) 553. MR0110669

[14] K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory (Second edition)", Springer-Verlag, 1990, page 96. MR1070716

[15] F. Lemmermeyer, "Reciprocity Laws: from Euler to Eisenstein", Springer-Verlag, 2000, page 210. MR1761696

[16] L. Mordell, "On the rational solutions of the indeterminate equations of the third and fourth degrees", Proc. Camb. Phil. Soc. 21 (1922) 179.
A. Weil, "L'arithmétique sur les courbes algébriques", Acta Math. 52 (1929) 281. MR1555278

[17] The PARI Group, PARI/GP version `2.11.4`, Univ. Bordeaux, 2019, pari.math.u-bordeaux.fr

[18] B. Birch and P. Swinnerton-Dyer, "Notes on elliptic curves (II)", Journal für die reine und angewandte Mathematik 218 (1965) 79, gdz.sub.uni-goettingen.de

[19] V. Kolyvagin, "Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a class of Weil curves", Math. USSR, Izv. 32 (1989) 523, wstein.org, MR0954295

[20] T. Nagell, "Solution de quelque problemes dans la theorie arithmetique des cubiques planes du premier genre", Wid. Akad. Skrifter Oslo I (1935), Nr. 1.
E. Lutz, "Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adic", J. Reine Angew. Math. 177 (1937) 431. MR1581558

[21] B. Mazur, "Rational isogenies of prime degree", Inventiones Mathematicae 44, 129 (1978), eudml.org/doc/142524, MR0482230

[22] The LMFDB Collaboration, The L-functions and Modular Forms Database, 2021, lmfdb.org/EllipticCurve/Q

[23] D. S. Kubert, "Universal bounds on the torsion of elliptic curves", Proc. London Math. Soc., 33 (1976) 193, citeseerx.ist.psu.edu

[24] M. S. Reichert, "Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields", Mathematics of Computation 46 (1986) 637, ams.org/journals/mcom, MR0829635

[25] A. O. L. Atkin and F. Morain, "Finding suitable curves for the elliptic curve method of factorization", Mathematics of Computation 60 (1993) 399, ams.org/journals/mcom, MR1140645

[26] J. Battista, J. Bayless, D. Ivanov, and K. James, "Average Frobenius distributions for elliptic curves with nontrivial rational torsion", Acta Arithmetica 119 (2006) 81, eudml.org/doc/278566, MR2163519

[27] P. Haggmark, "On an unsolved question concerning the Diophantine equation $Ax^3 + By^3 = C$," Arkiv for Math 1, 279 (1950), projecteuclid.org/euclid.afm/1485803959
W. Ljunggren, "On an improvement of a theorem of T. Nagell concerning the diophantine equation $Ax^3 + By^3 = C$," Math. Scandinavica 1, 297 (1953). MR0058617

[28] T. Nagell, "Remarques sur une classe d'équations indéterminées", Arkiv for Math 8, 199 (1969), projecteuclid.org/euclid.afm/1485894417

[29] A. Bremner and R. K. Guy, "Two more representation problems," Proc. of the Edinburgh Math. Soc. 40, 1 (1997), cambridge.org/core/journals, MR1437807

Bogdan A. Dobrescu
Particle Theory Department
Fermilab
Batavia, IL 60510
USA
E-mail address: bdob@fnal.gov

Patrick J. Fox
Particle Theory Department
Fermilab
Batavia, IL 60510
USA
E-mail address: pjfox@fnal.gov

Received September 30, 2021
Accepted March 8, 2022