International Journal of Number Theory
Vol. 18, No. 9 (2022) 1929–1955

DOI: 10.1142/S1793042122500993

World Scientific
www.worldscientific.com

Cyclic cubic extensions of $\mathbb{Q}$

Dipramit Majumdar
Department of Mathematics
Indian Institute of Technology Madras
Chennai 600036, India
dipramit@gmail.com

B. Sury*
Stat-Math Unit, Indian Statistical Institute
8th Mile Mysore Road, Bangalore 560059, India
surybang@gmail.com

Received 20 July 2021
Revised 19 February 2022
Accepted 20 February 2022
Published 25 April 2022

We determine the irreducible trinomials $X^3 - aX + b$ for integers a, b which generate precisely all possible Galois extensions of degree 3 over $\mathbb{Q}$. The proof, although involved, is elementary and one can parametrize all these polynomials explicitly. As an accidental by-product of the results, we prove that infinitely many primes congruent to 1 or -1 mod 9 are sums of two rational cubes - thereby, giving the first unconditional result on a classical open problem.

Keywords: Cubic Galois extensions; level raising and lowering maps; Diophantine equations; primes as sums of two cubes.

Mathematics Subject Classification 2020: 11D41, 12F05

1. Introduction

Let K be a Galois extension of $\mathbb{Q}$ of degree 3. Then, we can identify $K \cong \frac{\mathbb{Q}[X]}{(X^3-aX+b)}$ for some irreducible polynomial $X^3 - aX + b \in \mathbb{Z}[X]$ whose discriminant $4a^3 - 27b^2$ is a perfect square.

The aim of this paper is to explicitly describe the irreducible trinomials which give all the cubic Galois extensions of $\mathbb{Q}$. *This is done in the main Theorem* 4.6 *at the end.* It is surprising that this seems to have been not done before.

A classical open problem asks for a classification of all cube-free natural numbers which can be expressed as sums of cubes of two rational numbers. *As an accidental*

*Corresponding author.

by-product of our main result, we prove that infinitely primes congruent to ± 1 *modulo* 9 *can be expressed as a sum of two rational cubes.* Our proof seems to be the first unconditional one.

We call two polynomials $f(X) = X^3 - a_1X + b_1 \in \mathbb{Z}[X]$ and $g(X) = X^3 - a_2X + b_2 \in \mathbb{Z}[X]$ to be **equivalent** if there exists a rational number $q \in \mathbb{Q}^*$ such that $a_2 = q^2a_1$ and $b_2 = q^3b_1$. Note that $\mathrm{Disc}(g) = q^6\mathrm{Disc}(f)$. The aim of this paper is to find all irreducible polynomials $f(X) = X^3 - aX + b \in \mathbb{Z}[X]$ (up to equivalence) whose discriminant is a perfect square. Since we are only interested in polynomials up to equivalence, we need to find all the irreducible trinomials $f(X) = X^3 - aX + b \in \mathbb{Z}[X]$ each of which satisfies the following conditions:

(1) There exists an integer c such that $\mathrm{Disc}(f) = 4a^3 - 27b^2 = c^2 \neq 0$.
(2) $D = \mathrm{GCD}(a, b)$ is cube-free and, for every prime number ℓ such that $\ell^2 \mid D$, we have $\ell^3 \nmid b$.

We briefly explain why the study of cubic Galois extensions of $\mathbb{Q}$ reduces to the study of polynomials of the form $X^3 - aX + b$ satisfying the above two conditions. Note first that by a linear change of variables, a cubic irreducible polynomial over $\mathbb{Q}$ can be taken to be of the form $X^3 + uX + v$ for rational u, v and a further scaling by an integer w, where w is a common denominator for u and v, generates the same field with a primitive element whose minimal polynomial is of the form $X^3 - aX + b$ for integers a, b. Condition (1) arises as the Galois group of a cubic polynomial is cyclic, of order 3, if it is contained in the alternating group A_3 - which happens if and only if the discriminant is a perfect square ([5, Corollary 12.4]). Condition (2) arises because if ℓ is a prime such that $\ell^2 \mid \mathrm{GCD}(a, b)$ and $\ell^3 \mid b$, then the polynomial $X^3 - aX + b$ is equivalent to the polynomial $X^3 - (a/\ell^2)X + (b/\ell^3)$.

We write (a, b) for the GCD of a, b. Let us note that the determination of cubic trinomials $f(X)$ whose discriminant is a perfect square reduces to integral solutions $(\sqrt{\mathrm{Disc}(f)}, b, a)$ of $x^2 + 27y^2 = 4z^3$.

Let X_1 denote the affine curve $x^2 + 27y^2 = 4z^3$ and let

$$X_1^D(\mathbb{Z}) = \{(x, y, z) \in \mathbb{Z}^3 \mid x^2 + 27y^2 = 4z^3, xyz \neq 0, (y, z) = D\}.$$

For a cube-free natural number D, in view of property (2) above, we define

$$X_1^D(\mathbb{Z})^* = \{(x, y, z) \in X_1^D(\mathbb{Z}) : \ell^2 | D \Rightarrow \ell^3 \nmid y \ \forall \,\text{prime}\ \ell\}.$$

We observe that if D is square-free, then $X_1^D(\mathbb{Z}) = X_1^D(\mathbb{Z})^*$. Note that $(x, y, z) \in X_1^D(\mathbb{Z})^*$ gives us a trinomial $X^3 - zX + y$ which satisfies conditions (1) and (2). As we vary $(x, y, z) \in X_1^D(\mathbb{Z})^*$ for all cube-free natural numbers D, the irreducible trinomials $X^3 - zX + y$ give us all irreducible trinomials in $\mathbb{Z}[X]$ (up to equivalence) whose discriminant is a perfect square. Thus, we start by understanding the sets $X_1^D(\mathbb{Z})^*$.

We say a cube-free natural number D is **admissible** if $X_1^D(\mathbb{Z})^*$ is non-empty. We will show that D is admissible if, and only if, $D = D_1$ or $9D_1$ where either $D_1 = 1$ or each prime factor of D_1 is congruent to 1 mod 3.

So, we restrict our study to $X_1^D(\mathbb{Z})^*$ for admissible D.

Observing that any solution $(x, y, z) \in X_1^D(\mathbb{Z})$ gives us a solution (X, Y, Z) of $X^2 + 27Y^2 = 4DZ^3$ with $(Y, Z) = 1$ (where $x = DX, y = DY, z = DZ$), we let X_D denote the affine curve $X^2 + 27Y^2 = 4DZ^3$ for any admissible D. We think X_D as "level curves" and define

$$X_D^1(\mathbb{Z}) = \{(x, y, z) \in \mathbb{Z}^3 : xyz \neq 0, x^2 + 27y^2 = 4Dz^3, (y, z) = 1\}.$$

Then, we have a bijection from $X_1^D(\mathbb{Z}) \to X_D^1(\mathbb{Z})$ given by $(x, y, z) \mapsto (\frac{x}{D}, \frac{y}{D}, \frac{z}{D})$. Moreover, this map induces a bijection from $X_1^D(\mathbb{Z})^*$ to $X_D^1(\mathbb{Z})^*$, where

$$X_D^1(\mathbb{Z})^* = \{(x, y, z) \in X_D^1(\mathbb{Z}) : \ell^2 | D \Rightarrow \ell \nmid y \ \forall \, \text{prime } \ell\}.$$

We study the sets $X_D^1(\mathbb{Z})^*$; note that $X_D^1(\mathbb{Z}) = X_D^1(\mathbb{Z})^*$ if D is square-free.

We observe that, for an admissible D with $3 \nmid D$, the solutions of $X^2 + 27Y^2 = 4DZ^3$ are related in a many-to-one fashion with those of $X^2 + 3Y^2 = 4DZ^3$ - here, certain subtleties arise as follows:

When (x, y, z) is a solution to the first equation where $3 \mid z$, there are two solutions $(x, 3y, z)$ and $(y, x/9, z/3)$ for the latter equation.

Also, if (x, y, z) is a solution to the latter equation and $3 \mid y$, we get two solutions $(x, y/3, z)$ and $(9y, x, 3z)$ of the former equation.

Let Y_D denote the affine curve $X^2 + 3Y^2 = 4DZ^3$. Similar to the case of the affine curve X_D, we define

$$Y_D^1(\mathbb{Z}) = \{(x, y, z) \in \mathbb{Z}^3 : xyz \neq 0, x^2 + 3y^2 = 4Dz^3, (y, z) = 1\};$$

$$Y_D^1(\mathbb{Z})^* = \{(x, y, z) \in Y_D^1(\mathbb{Z}) : \ell^2 | D \Rightarrow \ell \nmid y \ \forall \, \text{prime } \ell\}.$$

In Sec. 2, for admissible D with $3 \nmid D$, we obtain $X_D^1(\mathbb{Z})^*$ in terms of $Y_D^1(\mathbb{Z})^*$. Also, for an admissible integer of the form $9D$, in Sec. 2, we give a bijection between $Y_D^1(\mathbb{Z})$ and $X_{9D}^1(\mathbb{Z})$. As a consequence, this enables us to identify $X_{9D}^1(\mathbb{Z})^*$ with a certain subset of $Y_D^1(\mathbb{Z})^*$. Therefore, we need to study $Y_D^1(\mathbb{Z})^*$ for admissible integers D with $3 \nmid D$.

In the study of $Y_D^1(\mathbb{Z})^*$, the case $D = 1$ is easy to deal with. The solutions are obtained explicitly by reducing the equation $X^2 + 3Y^2 = 4Z^3$ to the equation $x^2 - 3xy + 3y^2 = z^3$ that is quickly solved using the arithmetic of the ring $\mathbb{Z}[\omega]$, where ω is a primitive third root of unity. A detailed proof of this can be found in [1, Proposition 14.2.1(2)].

In Sec. 3, we construct $Y_D^1(\mathbb{Z})^*$ from $Y_1^1(\mathbb{Z})$ using maps between the integral points of curves of the form $X^2 + 3Y^2 = 4DZ^3$ for varying D and keeping track of the GCDs of Y and Z. These maps roughly "trade off" the GCD of (Y, Z) with a coefficient of the Z^3 term. Informally, we call these fundamental maps "level-raising" and "level-lowering". As the book-keeping is somewhat involved, it is convenient to define and study the maps abstractly.

Keeping track of the bookkeeping in Secs. 2 and 3, we determine in Sec. 4, all the irreducible trinomials (up to equivalence) whose discriminant is a perfect square.

In Sec. 5, we relate integers expressible as sum of rational cubes with integral solutions of $x^2 + 27y^2 = 4z^3$ and as a consequence we prove that infinitely many primes congruent to ± 1 modulo 9 can be expressed as a sum of two rational cubes.

To summarize the flow of the paper, we make a few remarks. The set of solutions of $x^2 + 27y^2 = 4z^3$ with a given $(y, z) = D$ is connected naturally to the study of solutions of $x^2 + 3y^2 = 4z^3$ with the same $(y, z) = D$ (in a slightly subtle way - see Lemma 2.10). The main work consists of constructing the relevant part of the set of solutions of $x^2 + 3y^2 = 4z^3$ with $\gcd(y, z) = D$ (denoted by $Y_D^1(\mathbb{Z})^*$) from the set of solutions of $x^2 + 3y^2 = 4z^3$ with $\gcd(y, z) = 1$, using level-changing maps. It seems to us that if we directly perform the various level-changing transformations within the sets of solutions of $x^2 + 27y^2 = 4z^3$ with various (y, z)'s, and try to bypass the equation $x^2 + 3y^2 = 4z^3$, it is artificial, and we are not able to ensure that all points are obtained. Hence, we are led to considering the level sets $Y_D^1(\mathbb{Z})^*$.

Theorem 4.6 *gives a complete list of irreducible trinomials which generate all possible cubic Galois extensions of* $\mathbb{Q}$.

For convenience, we put down here a summary of notation that will appear often in this paper.

- $X_1^D(\mathbb{Z}) = \{(x, y, z) \in \mathbb{Z}^3 : xyz \neq 0, x^2 + 27y^2 = 4z^3, (y, z) = D\}$.
- $X_1^D(\mathbb{Z})^* = \{(x, y, z) \in X_1^D(\mathbb{Z}) : \ell^2 | D \Rightarrow \ell^3 \nmid y \ \forall \text{ prime } \ell\}$.
- $X_D^1(\mathbb{Z}) = \{(x, y, z) \in \mathbb{Z}^3 : xyz \neq 0, x^2 + 27y^2 = 4Dz^3, (y, z) = 1\}$.
- $X_D^1(\mathbb{Z})^* = \{(x, y, z) \in X_D^1(\mathbb{Z}) : \ell^2 | D \Rightarrow \ell \nmid y \ \forall \text{ prime } \ell\}$.
- $Y_D^1(\mathbb{Z}) = \{(x, y, z) \in \mathbb{Z}^3 : xyz \neq 0, x^2 + 3y^2 = 4Dz^3, (y, z) = 1\}$.
- $Y_D^1(\mathbb{Z})^* = \{(x, y, z) \in Y_D^1(\mathbb{Z}) : \ell^2 | D \Rightarrow \ell \nmid y \ \forall \text{ prime } \ell\}$.

The idea is to define "level-changing" maps between these sets and determine the sets $X_1^D(\mathbb{Z})^* = \{(x, y, z) \in X_1^D(\mathbb{Z}) : \ell^2 | D \Rightarrow \ell^3 \nmid y \ \forall \text{ prime } \ell\}$ from $Y_1^1(\mathbb{Z}) = \{(x, y, z) \in \mathbb{Z}^3 : xyz \neq 0, x^2 + 3y^2 = 4z^3, (y, z) = 1\}$; the latter set can be written down explicitly.

2. Construction of $X_1^1(\mathbb{Z})$ and $X_1^9(\mathbb{Z})^*$

Let X_1 be the affine curve $X^2 + 27Y^2 = 4Z^3$ as defined in the introduction. We define the set of trivial integral zeroes of X_1 by

$$\begin{aligned} X_1^{\text{triv}}(\mathbb{Z}) &= \{(x_0, y_0, z_0) \in X_1(\mathbb{Z}) | x_0 y_0 z_0 = 0\} \\ &= \{(0, \pm 2t^3, 3t^2), (\pm 2t^3, 0, t^2) \mid t \in \mathbb{Z}\}. \end{aligned}$$

Note that if $(x_0, y_0, z_0) \in X_1^{\text{triv}}(\mathbb{Z})$, then $X^3 - z_0 X + y_0$ is reducible. As we are interested in irreducible trinomials (up to equivalence) with perfect square discriminant, we study the sets $X_1^D(\mathbb{Z})^* = \{(x, y, z) \in X_1^D(\mathbb{Z}) : \ell^2 | D \Rightarrow \ell^3 \nmid y \ \forall \text{prime } \ell\}$ as D vary over cube-free integers.

We first find all cube-free integers D for which the set $X_1^D(\mathbb{Z})^*$ can possibly be non-empty. Towards that, we recall the following elementary fact. We include a proof here.

Lemma 2.1. *Let $p \geq 5$ be an odd prime. Then there exists integer u and v such that $p = u^2 + 3v^2$ if and only if, $p \equiv 1 \pmod 3$. Also, u and v above are unique up to sign, and $(u, 3v) = 1$. Moreover, any prime $p \equiv 1$ mod 3 is expressible as $s^2 - st + t^2$ for positive integers s, t and the expression $p = u^2 + 3v^2$ has the unique positive solution $u = s + \frac{t}{2}, v = \frac{t}{2}$ when s is odd and t is even and $u = \frac{s+t}{2}, v = \frac{|s-t|}{2}$ when s, t are odd. Further, if an integer N is expressible in the form $a^2 + 3b^2$ with $(a, 3b) = 1$, then its odd prime factors are of the form $3k + 1$.*

Proof. Clearly, if $p \neq 3$ is of the form $x^2 + 3y^2$, then it is 1 mod 3. Conversely, let $p \equiv 1$ mod 3 be a prime. As 3 divides $|\mathbf{F}_p^*|$ there exists an element of order 3 in the cyclic group $\mathbf{F}_p^*$. That is, there exists an integer $a \not\equiv 1$ mod p but $a^3 \equiv 1$ mod p. Thus, p divides a^2+a+1 so that p divides $|-a+\omega|^2$ where ω is a primitive cube root of unity. Clearly, p is not irreducible (as it is not prime) in the unique factorization domain $\mathbf{Z}[\omega]$. Hence $p = (a + b\omega)(c + d\omega)$ with each factor a non-unit, which gives $p = |a + b\omega|^2 = a^2 - ab + b^2$. Therefore, either a, b are both odd or one of them (say a) is odd and the other even, In the first case, $p = ((a + b)/2)^2 + 3((a - b)/2)^2$ and, in the second case, $p = (a - b/2)^2 + 3(b/2)^2$. This completes the proof of the first statement. The fact that $(u, 3v) = 1$ is obvious.

To prove uniqueness (up to sign), let $p = u_1^2 + 3v_1^2 = u_2^2 + 3v_2^2$. Now

$$(u_1v_2 - v_1u_2)(u_1v_2 + v_1u_2) = u_1^2v_2^2 - v_1^2u_2^2 \equiv -v_1^2(u_2^2 + 3v_2^2) \equiv 0 \pmod p.$$

Thus, either $p \mid (u_1v_2 - v_1u_2)$ or $p \mid (u_1v_2 + v_1u_2)$.

If $p \mid (u_1v_2-v_1u_2)$, then $p \mid (u_1(u_1v_2-v_1u_2)-pv_2)$; that is, $p \mid -v_1(u_1u_2+3v_1v_2)$. Hence $p \mid (u_1u_2 + 3v_1v_2)$ as $(p, v_1) = 1$. Since

$$1 = \left(\frac{u_1u_2 + 3v_1v_2}{p}\right)^2 + 3\left(\frac{u_1v_2 - v_1u_2}{p}\right)^2,$$

we get $\frac{u_1v_2-v_1u_2}{p} = 0$ and $\frac{u_1u_2+3v_1v_2}{p} = \pm 1$. Thus, $u_1v_2 = u_2v_1$ and $u_1u_2 + 3v_1v_2 = \pm p$. So, $\pm pu_1 = u_1^2u_2 + 3v_1u_1v_2 = (u_1^2 + 3v_1^2)u_2 = pu_2$.

We conclude that $u_1 = \pm u_2$ and $v_1 = \pm v_2$.

The case $p \mid (u_1v_2 + v_1u_2)$ is similar. This concludes the proof of uniqueness of u, v in the expression of a prime $p = u^2 + 3v^2$ (up to sign).

Finally, let $N = a^2 + 3b^2$ with $(a, 3b) = 1$. Let p be an odd prime such that $p \mid N$. Since $(a, 3b) = 1$, we have $p \neq 3$ and $p \nmid ab$. since $a^2 + 3b^2 \equiv 0 \pmod p$, we see that $-3 \equiv \left(\frac{a}{b}\right)^2 \pmod p$, that is $\left(\frac{-3}{p}\right) = 1$. From the quadratic reciprocity law, it follows that $p \equiv 1 \pmod 3$. □

Proposition 2.2. *Let D be a cube-free integer. Consider the set $X_1^D(\mathbb{Z})^* = \{(x, y, z) \in X_1^D(\mathbb{Z}) : \ell^2 | D \Rightarrow \ell^3 \nmid y \ \forall \text{prime } \ell\}$ where $X_1^D(\mathbb{Z}) = \{(x, y, z) \in \mathbb{Z}^3 :$*

$xyz \neq 0, x^2 + 27y^2 = 4z^3, (y,z) = D\}$. *If a prime* $\ell \equiv 2 \pmod 3$ *divides* D, *then* $X_1^D(\mathbb{Z})^*$ *is empty.*

Proof. Let $(x_0, y_0, z_0) \in X_1^D(\mathbb{Z})^*$. We divide the proof in two cases.

Case I. $\ell = 2$.

Write $y_0 = 2y_1, z_0 = 2z_1$, this implies $2 \mid x_0$. Write $x_0 = 2x_1$. Simplifying, we get

$$x_1^2 + 27y_1^2 = 8z_1^3.$$

Thus $x_1^2 + 27y_1^2 \equiv 0 \pmod 8$. For any integer a, we have $a^2 \equiv 0, 1, 4 \pmod 8$. Thus, this implies either $x_1 \equiv y_1 \equiv 0 \pmod 4$ or $x_1 \equiv y_1 \equiv 2 \pmod 4$.

In the first case, $4 \mid x_1$ and $4 \mid y_1$ implies $2 \mid z_1$. Thus, $4 \mid (y_0, z_0) = D$ and $8 \mid y_0$ which implies $(x_0, y_0, z_0) \notin X_1^D(\mathbb{Z})^*$.

In the second case, writing $x_1 = 2(2r+1)$ and $y_1 = 2(2s+1)$, we obtain

$$(2r+1)^2 + 27(2s+1)^2 = 2z_1^3.$$

Since the left-hand side is divisible by 4, this implies z_1 is even. Writing $z_1 = 2t$ we obtain

$$(2r+1)^2 + 27(2s+1)^2 = 16t^3,$$

which is not possible, as right-hand side $\equiv 0 \pmod 8$ but left-hand side $\equiv 4 \pmod 8$.

Case II. $2 < \ell \equiv 2 \pmod 3$.

The proof of Lemma 2.1 implies that $x^2 + 3y^2 = 0$ has no solution other than $(0,0) \in \mathbb{F}_\ell^2$.

Suppose that $X^2 + 27Y^2 = 4Z^3$ has a non-trivial solution (x_0, y_0, z_0) with GCD $(y_0, z_0) = D$. If $\ell \mid y_0$ and $\ell \mid z_0$, then $\ell \mid x_0$. Writing $x_0 = \ell x_1, y_0 = \ell y_1, z_0 = \ell z_1$ and simplifying we see

$$x_1^2 + 27y_1^2 = 4\ell z_1^3 \text{ hence } x_1^2 + 3(3y_1)^2 = 0 \pmod \ell.$$

Hence $(x_1, 3y_1) = (0,0) \in \mathbb{F}_\ell^2$, that is $\ell \mid x_1$ and $\ell \mid y_1$. This implies $\ell^2 \mid D$ and $\ell \mid z_1$. Writing $x_1 = \ell x_2, y_1 = \ell y_2, z_1 = \ell z_2$ and simplifying, we see that

$$x_2^2 + 27y_2^2 = 4\ell^2 z_2^3 \text{ hence } x_2^2 + 3(3y_2)^2 = 0 \pmod \ell.$$

Again by a similar argument we see that $\ell \mid y_2$, hence $(x_0, y_0, z_0) \notin X_1^D(\mathbb{Z})^*$. □

Proposition 2.3. *Let* D *be a cube-free integer. If* $3 \mid\mid D$, *then* $X_1^D(\mathbb{Z})^*$ *is empty.*

Proof. Suppose $(x_0, y_0, z_0) \in X_1^D(\mathbb{Z})^*$. We see that $3 \mid z_0$ implies $27 \mid x_0^2$, hence $9 \mid x_0$. Now $9 \mid x_0$ and $3 \mid y_0$ implies $81 \mid z_1^3$, hence $9 \mid z_0$. Next we see that $3 \mid y_0$ and $9 \mid z_0$ implies $3^5 \mid x_0^2$, hence $3^3 \mid x_0$. Lastly, note that $3^3 \mid x_0$ and $9 \mid z_0$ implies $3^6 \mid 27y_0^2$, hence $9 \mid y_0$. Thus, we see that 9 divides both y_0 and z_0, hence $9 \mid D$, which contradicts the fact that $3 \mid\mid D$. □

In view of the above two propositions when our set $X_1^D(\mathbb{Z})^*$ is empty, it is meaningful to consider the following integers D only.

Definition 2.4. (i) We call a natural number D **admissible** if it is cube-free and of the form D_1 or $9D_1$, where $D_1 = 1$ or all the prime factors of D_1 are congruent to 1 modulo 3.

(ii) For admissible D, we consider the curve $X_D : X^2+27Y^2 = 4DZ^3$. As mentioned in the introduction, let

$$X_D^1(\mathbb{Z}) = \{(x, y, z) \in \mathbb{Z}^3 : xyz \neq 0, x^2 + 27y^2 = 4Dz^3, (y, z) = 1\};$$

$$X_D^1(\mathbb{Z})^* = \{(x, y, z) \in X_D^1(\mathbb{Z}) : \ell^2 | D \Rightarrow \ell \nmid y \ \forall \text{ prime } \ell\}.$$

We observe now that the sets $X_D^1(\mathbb{Z})$ and $X_D^1(\mathbb{Z})^*$ are in natural bijection, respectively, with the sets $X_1^D(\mathbb{Z})$ and $X_1^D(\mathbb{Z})^*$.

Lemma 2.5. *The map* $\theta_D : X_D^1(\mathbb{Z}) \to X_1^D(\mathbb{Z})$ *given by* $(x, y, z) \mapsto (Dx, Dy, Dz)$ *is a bijection and restricts to a bijection from* $X_D^1(\mathbb{Z})^*$ *to* $X_1^D(\mathbb{Z})^*$.

Proof. Indeed, note that if $(x, y, z) \in X_D^1(\mathbb{Z})$, then $(Dx)^2 + 27(Dy)^2 = D^2(x^2 + 27y^2) = D^2(4Dz^3) = 4(Dz)^3$, hence $(Dx, Dy, Dz) \in X_1(\mathbb{Z})$. Also since $(y, z) = 1$, this implies $(Dy, Dz) = D$, hence $(Dx, Dy, Dz) \in X_1^D(\mathbb{Z})$. Also note that if D is an admissible integer, then $(x, y, z) \in X_D^1(\mathbb{Z})^*$ if and only if $(Dx, Dy, Dz) \in X_1^D(\mathbb{Z})^*$.

Conversely, suppose $(x', y', z') \in X_1^D(\mathbb{Z})$. Then $(y', z') = D$ and hence D divides x', y' and z'. Define the map

$$\theta_D^{-1} : X_1^D(\mathbb{Z}) \to X_D^1(\mathbb{Z}); \quad (x', y', z') \mapsto \left(\frac{x'}{D}, \frac{y'}{D}, \frac{z'}{D}\right).$$

This is evidently the map θ_D^{-1} and maps $X_1^D(\mathbb{Z})^*$ to $X_D^1(\mathbb{Z})^*$.

We conclude that θ_D defines a bijection from $X_D^1(\mathbb{Z})$ to $X_1^D(\mathbb{Z})$ and restricts to a bijection from $X_D^1(\mathbb{Z})^*$ onto $X_1^D(\mathbb{Z})^*$. □

2.1. *A related curve*

For an admissible integer D such that $3 \nmid D$, we consider the level curve $Y_D : X^2 + 3Y^2 = 4DZ^3$. As before, we define

$$Y_D^1(\mathbb{Z}) = \{(x, y, z) \in \mathbb{Z}^3 : xyz \neq 0, x^2 + 3y^2 = 4Dz^3, (y, z) = 1\};$$

$$Y_D^1(\mathbb{Z})^* = \{(x, y, z) \in Y_D^1(\mathbb{Z}) : \ell^2 | D \Rightarrow \ell \nmid y \ \forall \text{prime } \ell\}.$$

Lemma 2.6. *Let* D *be an admissible integer with* $3 \nmid D$. *Then the map*

$$\delta_D : Y_D^1(\mathbb{Z}) \to X_{9D}^1(\mathbb{Z}) \quad \textit{given by } \delta(x, y, z) = (3x, y, z)$$

defines a bijection. We remark that the assumption $3 \nmid D$ *ensures that* $9D$ *is admissible.*

Proof. A simple calculation shows that $(x, y, z) \in Y_D^1(\mathbb{Z})$ implies $(3x, y, z) \in X_{9D}^1(\mathbb{Z})$.

Conversely, suppose that $(x, y, z) \in X_{9D}^1(\mathbb{Z})$. Then $x^2 + 27y^2 = 36Dz^3$, hence $3 \mid x$. Again an easy calculation shows $(\frac{x}{3}, y, z) \in Y_D^1(\mathbb{Z})$. □

Corollary 2.7. *Let D be an admissible integer with $3 \nmid D$. Then the map δ_D above defines a bijection of*

$$S'_D = \{(x, y, z) \in Y_D^1(\mathbb{Z})^* \mid 3 \nmid y\}$$

with $X_{9D}^1(\mathbb{Z})^*$.

Proof. If $(x, y, z) \in S'_D$, then $\delta_D(x, y, z) = (3x, y, z) \in X_{9D}^1(\mathbb{Z})$. It is obvious that for a prime $\ell \equiv 1 \pmod 3$, $\ell^2 \mid D \iff \ell^2 \mid 9D$ and in this situation $\ell \nmid y$ as $(x, y, z) \in Y_D^1(\mathbb{Z})^*$. Moreover, $3 \nmid y$ as $(x, y, z) \in S'_D$. Hence $\delta_D(x, y, z) \in X_{9D}^1(\mathbb{Z})^*$.

Conversely, if $(a, b, c) \in X_{9D}^1(\mathbb{Z})^* \subset X_{9D}^1(\mathbb{Z})$, then for a prime $\ell \equiv 1 \pmod 3$, $\ell^2 \mid D \iff \ell^2 \mid 9D$ and in this situation $\ell \nmid b$ as $(a, b, c) \in X_{9D}^1(\mathbb{Z})^*$. Moreover, we have $3 \nmid b$. We conclude that $(\frac{a}{3}, b, c) \in S'_D$. □

We recall the easy parametrization of the set $Y_1^1(\mathbb{Z})$ as mentioned in the introduction.

Theorem 2.8 ([1, Proposition 14.2.1(2)]). *The equation $X^2 + 3Y^2 = 4Z^3$ in nonzero integers x, y and z with x and y coprime has two disjoint parametrizations*

$$(x, y, z) = ((s + t)(2s - t)(s - 2t), 3st(s - t), s^2 - st + t^2)$$

$$(x, y, z) = (\pm((s + t)^3 - 9st^2), s^3 - 3s^2t + t^3, s^2 - st + t^2),$$

where in both cases s and t are co-prime integers with $3 \nmid (s + t)$. The first parametrization corresponds to the case $6 \mid y$ and the second where 6 is coprime to y.

Using this we obtain the following description of $X_1^9(\mathbb{Z})^*$ as follows:

Theorem 2.9.

$$X_1^9(\mathbb{Z})^* = \{\pm 27((s + t)^3 - 9st^2), 9(s^3 - 3s^2t + t^3), 9(s^2 - st + t^2)\}$$

where s and t are co-prime integers with $3 \nmid (s + t)$.

Proof. Composition of the maps δ_9 and θ_9 gives us a bijection

$$\theta_9 \circ \delta_9 : S'_1 \to X_9^1(\mathbb{Z})^* \to X_1^9(\mathbb{Z})^* \text{ given by } (x, y, z) \mapsto (27x, 9y, 9z).$$

Since $S'_1 = \{(\pm((s + t)^3 - 9st^2), s^3 - 3s^2t + t^3, s^2 - st + t^2) \mid (s, t) = 1, 3 \nmid s + t\}$ the result follows. □

We are interested in determining the set $X_D^1(\mathbb{Z})^* = \{(x,y,z) \in \mathbb{Z}^3 : xyz \neq 0, x^2+27y^2 = 4Dz^3, (y,z) = 1, \ell^2|D \Rightarrow \ell \nmid y \ \forall \text{prime } \ell\}$ in terms of the set $Y_D^1(\mathbb{Z})^* = \{(x,y,z) \in \mathbb{Z}^3) : xyz \neq 0, x^2+3y^2 = 4Dz^3, (y,z) = 1, \ell^2|D \Rightarrow \ell \nmid y \ \forall \text{prime } \ell\}$.

Lemma 2.10. *Let D be an admissible integer with $3 \nmid D$. Then*

$$X_D^1(\mathbb{Z})^* = \{(9y,x,3z) \mid (x,y,z) \in Y_D^1(\mathbb{Z})^*\} \cup \left\{\left(x, \frac{y}{3}, z\right) \mid (x,y,z) \in Y_D^1(\mathbb{Z})^*, 3 \mid y\right\}.$$

Proof. Let us write $X_D^1(\mathbb{Z})^*$ as a disjoint union of the sets T_D and T'_D, where

$$T_D = \{(x,y,z) \in X_D^1(\mathbb{Z})^* \mid 3 \nmid z\}, \quad T'_D = \{(x,y,z) \in X_D^1(\mathbb{Z})^* \mid 3 \mid z\}.$$

First, we show there is a bijection between T_D and $S_D = \{(x,y,z) \in Y_D^1(\mathbb{Z})^* | 3|y\}$. We have a natural map $\beta_D : T_D \to S_D$ given by $\beta_D(x,y,z) = (x,3y,z)$. Note that it is essential that $3 \nmid D$ for the map β_D to make sense (if $3 \mid D$, then $9 \mid D$, which will imply that the set S_D is empty). We also have a natural map $\alpha_D : S_D \to T_D$ given by $\alpha_D(x,y,z) = (x, \frac{y}{3}, z)$. Observe that $\alpha_D \circ \beta_D = id_{T_D}$ and $\beta_D \circ \alpha_D = id_{S_D}$. As a consequence, we can identify T_D with $\alpha_D(S_D) = \{(x, \frac{y}{3}, z) \,|\, (x,y,z) \in Y_D^1(\mathbb{Z})^*, 3 \,|\, y\}$.

Now we will show that there is a bijection between T'_D and $Y_D^1(\mathbb{Z})^*$ as follows.

We define a map $\beta'_D : T'_D \to Y_D^1(\mathbb{Z})^*$ given by $\beta'_D(x,y,z) = (y, \frac{x}{9}, \frac{z}{3})$. To ensure that the map is well defined, we need to check

(i) $9 \mid x$, (ii) $\text{GCD}(\frac{x}{9}, \frac{z}{3}) = 1$ and (iii) if $\ell^2 \mid D$, then $\ell \nmid \frac{x}{9}$.

Now if $(x,y,z) \in X_D^1(\mathbb{Z})$ and $3 \mid z$, then it follows that $9 \mid x$. Moreover in this situation, it follows that if $\text{GCD}(\frac{x}{9}, \frac{z}{3}) = d > 1$, then $d \mid y$, which contradicts $\text{GCD}(y,z) = 1$. Further, as $(x,y,z) \in X_D^1(\mathbb{Z})^*$, it follows that if $\ell^2 \mid D$, then $\ell \nmid y$. Hence $\ell \nmid y^2 = (4D(\frac{z}{3})^3 - 3(\frac{x}{9})^2)$, which implies $\ell \nmid \frac{x}{9}$ (as $\ell \neq 3$). This shows that the map β'_D is well defined.

We also have a map $\alpha'_D : Y_D^1(\mathbb{Z})^* \to T'_D$ given by $\alpha'_D(x,y,z) = (9y,x,3z)$. To ensure that the map is well defined, we need to check

(i) $\text{GCD}(x,3z) = 1$ and (ii) if $\ell^2 \mid D$, then $\ell \nmid x$.

Note that if $(x,y,z) \in Y_D^1(\mathbb{Z})^*$ with $3 \mid x$, then $3 \mid z$ (as $3 \nmid D$), which in turn shows that $3 \mid y$, which contradicts $\text{GCD}(y,z) = 1$. This shows that $\text{GCD}(x,3z) = \text{GCD}(x,z) = d$ with $3 \nmid d$. Now if $\text{GCD}(x,z) = d > 1$, then $d^2 \mid 3y^2 = 4Dz^3 - x^2$ and hence $d \mid y$, which contradicts $\text{GCD}(y,z) = 1$. Thus $\text{GCD}(x,3z) = 1$. Moreover, as $(x,y,z) \in Y_D^1(\mathbb{Z})^*$, it follows that if $\ell^2 \mid D$, then $\ell \nmid y$. Hence ℓ does not divide $x^2 = (4Dz^3 - 27y^2)$ as ℓ^2 divides D and $\ell \neq 3$. This shows that the map α'_D is well defined.

Now observe that $\alpha'_D \circ \beta'_D = id_{T'_D}$ and $\beta'_D \circ \alpha'_D = id_{Y_D^1(\mathbb{Z})^*}$.

As a consequence, we can identify T'_D with $\alpha'_D(Y_D^1(\mathbb{Z})^*) = \{(9y,x,3z) \mid (x,y,z) \in Y_D^1(\mathbb{Z})^*\}$. This completes the proof of the lemma. □

Using the parametrization of $Y_1^1(\mathbb{Z})$ and Lemma 2.10 above, we obtain immediately

Theorem 2.11. *The set* $X_1^1(\mathbb{Z}) = \{(x,y,z) \in \mathbb{Z}^3 : xyz \neq 0, x^2+27y^2 = 4z^3, (y,z)=1\}$ *is given by the parametrizations*

$$\{(9(s^3-3s^2t+t^3), \pm((s+t)^3-9st^2), 3(s^2-st+t^2))\}$$
$$\cup\{(27st(s-t), (s+t)(2s-t)(s-2t), 3(s^2-st+t^2))\}$$
$$\cup\{((s+t)(2s-t)(s-2t), st(s-t), s^2-st+t^2)\},$$

where s *and* t *are coprime integers with* $3 \nmid (s+t)$.

Remark. We remark that the three sets that occur in the parametrization appearing in Theorem 2.11 are disjoint. To see this, note that

$$(s+t)(2s-t)(s-2t) = (s+t)(3s-(s+t))((s+t)-3t)$$
$$\equiv -(s+t)^3 \pmod 3 \quad \text{and}$$
$$s^3-3s^2t+t^3 = (s+t)^3-3(2s^2t+st^2 \equiv (s+t)^3 \pmod 3.$$

Thus, the condition $3 \nmid (s+t)$ implies $9 \,||\, 9(s^3-3s^2t+t^3)$ and $3 \nmid (s+t)(2s-t)(s-2t)$. This is equivalent to asserting that the first co-ordinate of an element is exactly divisible by 9 in the first parametric set, is divisible by 27 in the second parametric set, and is coprime to 3 in the third parametric set.

3. Integral Points on the Curve $X^2+3Y^2 = 4DZ^3$

Recall that Y_D denotes the affine curve $X^2+3Y^2 = 4DZ^3$. By $Y_D(\mathbb{Z})$ we denote the set of integral points on the affine curve Y_D, that is $Y_D(\mathbb{Z}) = \{(a,b,c) \in \mathbb{Z}^3 \mid a^2+3b^2 = 4Dc^3\}$. In this section, for a cube-free natural number D, we describe the set

$$Y_D^1(\mathbb{Z}) = \{(X,Y,Z) \in \mathbb{Z}^3 \mid X^2+3Y^2 = 4DZ^3, XYZ \neq 0, (Y,Z)=1\}.$$

We observe that if for a prime ℓ , $\ell^2 \mid D$ and $(x,y,z) \in Y_D^1(\mathbb{Z})$ with $\ell \mid y$, then $\ell \mid x$ and we have $(\frac{x}{\ell}, \frac{y}{\ell}, z) \in Y_{\frac{D}{\ell^2}}^1(\mathbb{Z})$.

Using this, we can inductively describe $Y_D^1(\mathbb{Z})$ as follows:

Assume that $3 \nmid D$. Write $D = \ell_1^2 \cdots \ell_r^2 D_1$, where D_1 is square-free with $\ell_1 \cdots \ell_r \nmid D_1$.

We have $Y_{D_1}^1(\mathbb{Z}) = Y_{D_1}^1(\mathbb{Z})^*$.

Now

$$Y_{\ell_1^2 D_1}^1(\mathbb{Z}) = \{(x,y,z) \in Y_{\ell_1^2 D_1}^1(\mathbb{Z}) \mid \ell_1 \nmid y\} \sqcup \{(x,y,z) \in Y_{\ell_1^2 D_1}^1(\mathbb{Z}) \mid \ell_1 \mid y\}$$
$$= Y_{\ell_1^2 D_1}^1(\mathbb{Z})^* \sqcup \{(\ell_1 x_1, \ell_1 y_1, z) \mid (x_1,y_1,z) \in Y_{D_1}^1(\mathbb{Z})^*, \ell_1 \nmid z\}.$$

For the last equality, we have used the fact that $\ell_1 \mid y$ implies $\ell_1 \mid x$ and $(\frac{x}{\ell_1}, \frac{y}{\ell_1}, z) \in Y^1_{D_1}(\mathbb{Z}) = Y^1_{D_1}(\mathbb{Z})^*$.

Proceeding in this manner, let $1 < B_1 \neq B_2 \neq \cdots \neq B_{2^r-1} \leq \ell_1 \cdots \ell_r$ be the set of divisors of $\ell_1 \cdots \ell_r$. We have

$$Y^1_D(\mathbb{Z}) = Y^1_D(\mathbb{Z})^* \sqcup_{i=1}^{2^r-1} \{(B_i x, B_i y, z) \mid (x, y, z) \in Y^1_{\frac{D}{B_i^2}}(\mathbb{Z})^*, B_i \nmid z\}.$$

Thus, for any cube-free integer D, with $3 \nmid D$, we can explicitly describe the set $Y^1_D(\mathbb{Z})$ if we know the set $Y^1_D(\mathbb{Z})^*$ for all cube-free integers D, with $3 \nmid D$.

We observe that for any cube-free integer D, with $3 \nmid D$, $(a, b, c) \in Y^1_D(\mathbb{Z})$ implies $3 \nmid c$. We can construct $Y^1_{3D}(\mathbb{Z})$ and $Y^1_{9D}(\mathbb{Z})$ from $Y^1_D(\mathbb{Z})$ as follows:

$$Y^1_{3D}(\mathbb{Z}) = \{(3b, a, c) \mid (a, b, c) \in Y^1_D(\mathbb{Z})\} \quad \text{and}$$
$$Y^1_{9D}(\mathbb{Z}) = \{(3a, 3b, c) \mid (a, b, c) \in Y^1_D(\mathbb{Z})\}.$$

Thus, it suffices to understand the sets $Y^1_D(\mathbb{Z})^*$ for all cube-free D, with $3 \nmid D$.

Proposition 3.1. *Let D be a cube-free integer, with $3 \nmid D$. If a prime $\ell \equiv 2 \pmod 3$ divides D, then $Y^1_D(\mathbb{Z})^*$ is empty.*

Proof. The proof is similar to that of Proposition 2.2; hence it is omitted. □

In view of the above discussion, we see that it is enough to understand the sets $Y^1_D(\mathbb{Z})^*$ for **admissible** integers D for which $3 \nmid D$. In the remaining part of the section, we describe how to obtain $Y^1_D(\mathbb{Z})^*$ from $Y^1_1(\mathbb{Z})$ using level raising and level lowering maps. We first describe the set $Y^1_p(\mathbb{Z})$ for a prime p of the form $3k + 1$. The case for general admissible D for which $3 \nmid D$ is similar, but more notationally involved.

Definition 3.2 (Level Raising by A Prime $p \equiv 1 \pmod 3$). Let p be a prime which is congruent to 1 modulo 3. Then, we can write p uniquely as $p = u^2 + 3v^2$ and $(u, 3v) = 1$ with $u, v > 0$. We define two-level raising maps by p as follows:

$$[p]^+ : Y^1_D(\mathbb{Z}) \to Y_{pD}(\mathbb{Z}) \quad \text{and} \quad [p]^- : Y^1_D(\mathbb{Z}) \to Y_{pD}(\mathbb{Z})$$

given by

$$[p]^+(x, y, z) = (ux + 3vy, uy - vx, z) \quad \text{and} \quad [p]^-(x, y, z) = (ux - 3vy, uy + vx, z).$$

The definition is justified by the following calculation:

$$(ux \pm 3vy)^2 + 3(uy \mp vx)^2 = (x^2 + 3y^2)(u^2 + 3v^2) = 4pDz^3.$$

Definition 3.3 (Level Lowering By A Prime $p \equiv 1 \pmod 3$). Let p be a prime which is congruent to 1 modulo 3. Then we can write p uniquely as $p = u^2 + 3v^2$ and $(u, 3v) = 1$ with $u, v > 0$. We define the level lowering map by p as

follows:

$$[p]_* : Y^1_{pD}(\mathbb{Z})^* \to Y_D(\mathbb{Z})$$

$$[p]_*(x,y,z) \mapsto \begin{cases} \left(\dfrac{ux-3vy}{p}, \dfrac{uy+vx}{p}, z\right) & \text{if } p \mid (uy+vx), \\ \left(\dfrac{ux+3vy}{p}, \dfrac{uy-vx}{p}, z\right) & \text{if } p \nmid (uy+vx). \end{cases}$$

The definition is justified as follows:
If $(x,y,z) \in Y^1_{pD}(\mathbb{Z})$, then

$$u^2y^2 - v^2x^2 \equiv -3v^2y^2 - v^2x^2 = -v^2(x^2+3y^2) = -4pDv^2z^3 \equiv 0 \pmod{p}.$$

Thus p divides either $(uy+vx)$ or $(uy-vx)$. Note that if $(x,y,z) \in Y^1_{pD}(\mathbb{Z})^*$ and p divides both of $uy+vx$ and $uy-vx$, then it implies that p divides both x and y. Hence if $p \mid D$, then $p^2 \mid pD$ and $p \mid y$ so that $(x,y,z) \notin Y^1_{pD}(\mathbb{Z})^*$. On the other hand, if p divides both x and y as above, and $p \nmid D$, then $p \mid z$. Hence $(x,y,z) \notin Y^1_{pD}(\mathbb{Z})$. So, we conclude that $(x,y,z) \in Y^1_{pD}(\mathbb{Z})^*$ implies p divides exactly one of $\{uy+vx, uy-vx\}$. If $p \mid (uy \pm vx)$, then p divides $u(uy \pm vx) - py = \pm v(ux \mp 3vy)$; hence $p \mid (ux \mp 3vy)$.

Finally, note that

$$\left(\frac{ux \mp 3vy}{p}\right)^2 + 3\left(\frac{uy \pm vx}{p}\right)^2 = \frac{1}{p^2}(u^2+3v^2)(x^2+3y^2) = 4Dz^3.$$

Lemma 3.4. *Let D be an admissible integer and $p \mid D$ be a prime (which is necessarily congruent to 1 modulo 3). Then, the level lowering map $[p]_*$ as defined in Definition 3.3 maps $Y^1_D(\mathbb{Z})^*$ to $Y^1_{\frac{D}{p}}(\mathbb{Z})^*$.*

Proof. Suppose $(x_0,y_0,z_0) \in Y^1_D(\mathbb{Z})^*$ and let $[p]_*(x_0,y_0,z_0) = (\tilde{x},\tilde{y},z_0)$. Suppose that $(\tilde{y},z_0) = d$, then $(\tilde{x},z_0) = d$, hence $d \mid \tilde{x}$ and $d \mid \tilde{y}$. Thus $d \mid (u\tilde{y} \mp v\tilde{x})$; in particular, $d \mid y_0$. Thus $d \mid (y_0,z_0) = 1$. So, $[p]_*(x_0,y_0,z_0) \in Y^1_{\frac{D}{p}}(\mathbb{Z})$. Note that $p^2 \nmid \frac{D}{p}$ as D is cube-free. Let $\ell_1 \neq p$ be a prime such that $\ell_1^2 \mid D$ and $(x_0,y_0,z_0) \in Y^1_D(\mathbb{Z})^*$, then $\ell_1 \nmid y_0$. Now, note that

$$u^2y_0^2 - v^2x_0^2 = py_0^2 - v^2(x_0^2+3y_0^2) = py_0^2 - 4Dv^2z_0^3 \equiv py_0^2 \neq 0 \pmod{\ell_1}.$$

Note that $\tilde{y}$ is either $(uy_0+vx_0)/p$ or $(uy_0-vx_0)/p$. Thus $\ell_1 \nmid \tilde{y}$. Hence $(\tilde{x},\tilde{y},z_0) \in Y^1_{\frac{D}{p}}(\mathbb{Z})^*$. □

Our aim is to construct $Y^1_D(\mathbb{Z})^*$ from $Y^1_1(\mathbb{Z})$ using level raising maps. For each prime divisors p of D, we apply p-level raising maps (twice if $p^2|D$). The main issue is to prove that we have constructed the whole $Y^1_D(\mathbb{Z})^*$. For this, we need to use the

level lowering maps. Now we study the image of the level lowering and level raising map.

We make some observations which will be proved to be valid in general in the proposition as follows:

Observe that the point $(-1,1,1) \in Y_1^1(\mathbb{Z})$ gives

$$[7]^+(-1,1,1) = (1,3,1), \quad [7]^-(-1,1,1) = (-5,1,1) \in Y_7^1(\mathbb{Z}),$$

moreover

$$[7]_* \circ [7]^+(-1,1,1) = [7]_* \circ [7]^-(-1,1,1) = (-1,1,1),$$

but

$$[7]^+ \circ [7]_*(1,3,1) = (1,3,1), \quad [7]^- \circ [7]_*(1,3,1) = (-5,1,1) \neq (1,3,1).$$

The point $(20,18,7) \in Y_1^1(\mathbb{Z})$ gives

$$[7]^+(20,18,7) = (94,16,7) \in Y_7^1(\mathbb{Z}),$$

$$[7]^-(20,18,7) = (-14,56,7) \in Y_7(\mathbb{Z}) \setminus Y_7^1(\mathbb{Z})$$

and we have

$$[7]^+ \circ [7]_*(94,16,7) = (94,16,7), [7]^- \circ [7]_*(94,16,7)$$
$$= (-14,56,7), [7]_* \circ [7]^+(20,18,7) = (20,18,7).$$

These observations are quite general in nature and the general case is proved in the proposition below. We remark that if $p^2 \mid D$, then pD is not an admissible integer, hence we are not concerned about the image of a point $(x_0,y_0,z_0) \in Y_D^1(\mathbb{Z})^*$ under level raising by p-map if $p^2 \mid D$.

Proposition 3.5. *Let D be an admissible integer, $p \equiv 1 \pmod 3$ be a prime. Let (x_0,y_0,z_0) be a point in $Y_D^1(\mathbb{Z})^*$.*

(1) *If $p \nmid Dz_0$, then both $[p]^{\pm}(x_0,y_0,z_0) \in Y_{pD}^1(\mathbb{Z})^*$.*
Otherwise, exactly one of the two points $[p]^+(x_0,y_0,z_0), [p]^-(x_0,y_0,z_0)$ belongs to $Y_{pD}^1(\mathbb{Z})^*$ if $p^2 \nmid D$.

(2) *If $p \mid D$, then exactly one of $\{[p]^+ \circ [p]_*(x_0,y_0,z_0), [p]^- \circ [p]_*(x_0,y_0,z_0)\}$ is (x_0,y_0,z_0).*

(3) *Suppose $p^2 \nmid D$. If $[p]^{\pm}(x_0,y_0,z_0) \in Y_{pD}^1(\mathbb{Z})^*$, then $[p]_* \circ [p]^{\pm}(x_0,y_0,z_0) = (x_0,y_0,z_0)$.*

Proof. For convenience of notation, let us write $[p]^{\pm}(x_0,y_0,z_0) = (x_1^{\pm}, y_1^{\pm}, z_0)$ and $[p]_*(x_0,y_0,z_0) = (\tilde{x},\tilde{y},z_0)$.

(1) First, consider the case $p \nmid D$. Suppose $\ell_1^2 \mid D$ (so $\ell_1 \neq p$ as we are in the case $p \nmid D$). Since $(x_0,y_0,z_0) \in Y_D^1(\mathbb{Z})^*$, we have $\ell_1 \nmid y_0$. We first show that $\ell_1 \nmid (y_1^+ y_1^-)$. Suppose $\ell_1 \mid y_1^{\pm}$, then ℓ_1 divides $4pDz_0^3 - 3(y_1^{\pm})^2 = (x_1^{\pm})^2$; thus, $\ell_1 \mid x_1^{\pm}$. Hence, ℓ_1 divides $uy_1^{\pm} \pm vx_1^{\pm} = py_0$, contradiction.

Thus, if $p \nmid D$ and $p \nmid z_0$, then it follows that both $(x_1^{\pm}, y_1^{\pm}, z_0) \in Y_{pD}^1(\mathbb{Z})^*$. We remark that the condition $p \nmid z_0$ is essential as otherwise from Eq. (1) it follows that $p \mid y_1^+ y_1^-$ and hence $p \mid (y_1^+, z_0)$ or $p \mid (y_1^-, z_0)$ which implies both $(x_1^{\pm}, y_1^{\pm}, z_0)$ cannot be in $Y_{pD}^1(\mathbb{Z})^*$.

Now suppose $p \mid Dz_0$ and $p^2 \nmid D$. Note that

$$y_1^+ y_1^- = u^2 y_0^2 - v^2 x_0^2 \equiv -v^2(x_0^2 + 3y_0^2) \equiv -4Dv^2 z_0^3 \equiv 0 \pmod{p}, \tag{1}$$

hence p divides at least one of y_1^+ and y_1^-. If $p \nmid D$, but $p \mid z_0$, then $[p]^{\pm}(x_0, y_0, z_0) \in Y_{pD}^1(\mathbb{Z})^*$ if and only if $p \nmid y_1^{\pm}$. If $p \mid y_1^+$ and $p \mid y_1^-$, then p divides $y_1^+ + y_1^- = 2uy_0$, which is not possible as $p \nmid u$ and $(y_0, z_0) = 1$. Thus, p divides exactly one of y_1^+ and y_1^-.

If $p \mid\mid D$, then $p^2 \mid\mid pD$. Now from the definition of $Y_{pD}^1(\mathbb{Z})^*$ it follows that $[p]^{\pm}(x_0, y_0, z_0) = (x_1^{\pm}, y_1^{\pm}, z_0) \in Y_{pD}^1(\mathbb{Z})^*$ if and only if $p \nmid y_1^{\pm}$. Now if $p \mid y_1^+$ and $p \mid y_1^-$, then p divides both $y_1^- + y_1^+ = 2uy_0$ and $y_1^- - y_1^+ = 2vx_0$. Thus, $p \mid x_0$ and $p \mid y_0$, which implies that p^2 divides $x_0^2 + 3y_0^2 = 4Dz_0^3$. This would mean that $p \mid z_0$ as $p^2 \nmid D$. Then $p \mid (y_0, z_0)$, contradiction. Hence, p divides exactly one of y_1^+ and y_1^-.

(2) As $p \mid D$, from Eq. (1) it follows that p divides exactly one of $y_1^- = uy_0 + vx_0$ and $y_1^+ = uy_0 - vx_0$. If $p \mid y_1^-$, then $\tilde{x} = \frac{x_1^-}{p}$ and $\tilde{y} = \frac{y_1^-}{p}$. We obtain

$$\begin{aligned}[p]^+ \circ [p]_*(x_0, y_0, z_0) &= [p]^+\left(\frac{x_1^-}{p}, \frac{y_1^-}{p}, z_0\right) = \left(\frac{ux_1^- + 3vy_1^-}{p}, \frac{uy_1^- - vx_1^-}{p}, z_0\right) \\ &= (x_0, y_0, z_0),\end{aligned}$$

$$\begin{aligned}[p]^- \circ [p]_*(x_0, y_0, z_0) &= [p]^-\left(\frac{x_1^-}{p}, \frac{y_1^-}{p}, z_0\right) = \left(\frac{ux_1^- - 3vy_1^-}{p}, \frac{uy_1^- + vx_1^-}{p}, z_0\right) \\ &= (x_0 - 6v\tilde{y}, y_0 + 2v\tilde{x}, z_0).\end{aligned}$$

Note that $\tilde{x}\tilde{y} \neq 0$ as $(\tilde{x}, \tilde{y}, z_0) \in Y_{\frac{D}{p}}^1(\mathbb{Z})^*$, hence $[p]^- \circ [p]_*(x_0, y_0, z_0) \neq (x_0, y_0, z_0)$. The case $p \mid y_1^+$ is similar.

(3) Suppose that $[p]^+(x_0, y_0, z_0) = (x_1^+, y_1^+, z_0) \in Y_{pD}^1(\mathbb{Z})^*$. Note that $uy_1^+ + vx_1^+ = py_0$ and $ux_1^+ - 3vy_1^+ = px_0$. As $p \mid (uy_1^+ + vx_1^+)$, we obtain $[p]_*(x_1^+, y_1^+, z_0) = (x_0, y_0, z_0)$. The case $[p]^-(x_0, y_0, z_0) \in Y_{pD}^1(\mathbb{Z})^*$ is similar. □

Lemma 3.6. *Let p and q be two distinct prime congruent to 1 modulo 3. Let $p = u_1^2 + 3v_1^2$ and $q = u_2^2 + 3v_2^2$. Let $u' = u_1u_2 - 3v_1v_2, v' = u_2v_1 + u_1v_2$ and $u'' = u_1u_2 + 3v_1v_2, v'' = u_2v_1 - u_1v_2$. We have*

$$\begin{aligned}[p]^+ \circ [p]^+(x_0, y_0, z_0) &:= [p]^{++}(x_0, y_0, z_0) \\ &= ((u_1^2 - 3v_1^2)x_0 + 6u_1v_1y_0, (u_1^2 - 3v_1^2)y_0 - 2u_1v_1x_0, z_0),\end{aligned}$$

$$\begin{aligned}
[p]^- \circ [p]^-(x_0,y_0,z_0) &:= [p]^{--}(x_0,y_0,z_0)\\
&= ((u_1^2-3v_1^2)x_0 - 6u_1v_1y_0, (u_1^2-3v_1^2)y_0 + 2u_1v_1x_0, z_0),\\
[p]^+ \circ [q]^+(x_0,y_0,z_0) &= [q]^+ \circ [p]^+(x_0,y_0,z_0) = (u'x_0+3v'y_0, u'y_0 - v'x_0, z_0),\\
[p]^+ \circ [q]^-(x_0,y_0,z_0) &= [q]^- \circ [p]^+(x_0,y_0,z_0) = (u''x_0+3v''y_0, u''y_0 - v''x_0, z_0),\\
[p]^- \circ [q]^+(x_0,y_0,z_0) &= [q]^+ \circ [p]^-(x_0,y_0,z_0) = (u''x_0-3v''y_0, u''y_0 + v''x_0, z_0),\\
[p]^- \circ [q]^-(x_0,y_0,z_0) &= [q]^- \circ [p]^-(x_0,y_0,z_0) = (u'x_0-3v'y_0, u'y_0 + v'x_0, z_0).
\end{aligned}$$

Proof. A straightforward calculation works. □

Remark 3.7. Observe that $(u_1^2-3v_1^2, 6u_1v_1) = 1$ and $(u_1^2-3v_1^2)^2+3(2u_1v_1)^2 = p^2$. This is the unique representation (up to sign) of p^2 as $\alpha^2+3\beta^2$ with $(\alpha, 3\beta) = 1$. Similarly, $(u', 3v') = (u'', 3v'') = 1$ and $u'^2+3v'^2 = u''^2+3v''^2 = pq$. Also, these are the only representations of pq (up to sign) as $\alpha^2+3\beta^2$ with $(\alpha, 3\beta) = 1$.

We also remark that for any $(x_0,y_0,z_0) \in Y_D^1(\mathbb{Z})$ (with $p \nmid D$), $[p]^+ \circ [p]^-(x_0,y_0,z_0) = [p]^- \circ [p]^+(x_0,y_0,z_0) = (px_0, py_0, z_0) \notin Y_{p^2D}^1(\mathbb{Z})^*$.

Lemma 3.8. *Let D be an admissible integer and $p \equiv 1 \pmod 3$ a prime such that $p \nmid D$. Let (x_0,y_0,z_0) be a point in $Y_D^1(\mathbb{Z})^*$. Then, $[p]^{++}(x_0,y_0,z_0) \in Y_{p^2D}^1(\mathbb{Z})^*$ if and only if $[p]^+(x_0,y_0,z_0) \in Y_{pD}^1(\mathbb{Z})^*$. Similarly, $[p]^{--}(x_0,y_0,z_0) \in Y_{p^2D}^1(\mathbb{Z})^*$ if and only if $[p]^-(x_0,y_0,z_0) \in Y_{pD}^1(\mathbb{Z})^*$.*

Proof. Let $(x_0,y_0,z_0) \in Y_D^1(\mathbb{Z})^*$. For convenience of notation, let us write $[p]^\pm(x_0,y_0,z_0) = (x_1^\pm, y_1^\pm, z_0)$ and $[p]^{\pm\pm}(x_0,y_0,z_0) = (x_2^\pm, y_2^\pm, z_0)$. Suppose ℓ_1 is a prime such that $\ell_1^2 \mid D$ (this necessarily mean $\ell_1 \neq p$). Then, $\ell_1 \nmid y_0$ by the definition of $Y_D^1(\mathbb{Z})^*$. We first show that $\ell_1 \nmid y_2^+y_2^-$. Suppose $\ell_1 \mid y_2^\pm$, then $\ell_1^2 \mid 4p^2Dz_0^3 - 3(y_2^\pm)^2 = (x_2^\pm)^2$, hence $\ell_1 \mid x_2^\pm$. As a consequence, ℓ_1 divides $(u^2-3v^2)y_2^\pm \pm 2uvx_2^\pm = p^2y_0$, a contradiction.

Now note that

$$\begin{aligned}
y_2^+y_2^- &= (u^2-3v^2)^2y_0^2 - (2uv)^2x_0^2 \equiv -(2uv)^2(x_0^2+3y_0^2)\\
&\equiv -4(2uv)^2Dz_0^3 \pmod p.
\end{aligned}$$

Thus if $p \nmid z_0$, then $p \nmid y_2^+y_2^-$, hence both $[p]^{++}(x_0,y_0,z_0), [p]^{--}(x_0,y_0,z_0) \in Y_{p^2D}^1(\mathbb{Z})^*$. Recall that (by Proposition 3.5) in this case both $[p]^\pm(x_0,y_0,z_0) \in Y_{p^2D}^1(\mathbb{Z})^*$.

Now suppose that $p \mid z_0$. Then $[p]^\pm(x_0,y_0,z_0) \in Y_{pD}^1(\mathbb{Z})^*$ if and only if $p \nmid y_1^\pm$, which is equivalent to $p \nmid x_1^\pm$. Then

$$y_2^\pm = (u^2-3v^2)y_0 \mp 2uvx_0 \equiv \mp 2v(ux_0 \pm 3vy_0) = \mp 2vx_1^\pm \pmod p.$$

Thus, if $p \mid z_0$, then $(x_2^{\pm}, y_2^{\pm}, z_0) \in Y^1_{p^2D}(\mathbb{Z})^*$ if and only if $p \nmid y_2^{\pm}$ which is equivalent to $p \nmid x_1^{\pm}$ which, in turn, is equivalent to $(x_1^{\pm}, y_1^{\pm}, z_0) \in Y^1_{pD}(\mathbb{Z})^*$. □

Lemma 3.9. *Let D be an admissible integer with $3 \nmid D > 1$. Then every element of $Y^1_D(\mathbb{Z})^*$ is the image of some element of $Y^1_1(\mathbb{Z})$. More precisely, let $R_D = \{(u_j, v_j) \in \mathbb{Z}^2 \mid D = u_j^2 + 3v_j^2, (u_j, 3v_j) = 1, u_j > 0, v_j > 0\}$. Then every element of $Y^1_D(\mathbb{Z})^*$ is of the form $(u_j x_0 \pm 3v_j y_0, u_j y_0 \mp v_j x_0, z_0)$ for some $(x_0, y_0, z_0) \in Y^1_1(\mathbb{Z})$ and some $(u_j, v_j) \in R_D$.*

Proof. The lemma follows from the previous lemmata in this section but, in order to make the proof more transparent, we give precise details here. Note that D is a cube-free integer > 1 which is a product of primes of the form $3k + 1$. It suffices to prove the more precise assertion:

Claim. Every element of $Y^1_D(\mathbb{Z})^*$ is of the form $(ux_0 \pm 3vy_0, uy_0 \mp vx_0, z_0)$ for some $(x_0, y_0, z_0) \in Y^1_1(\mathbb{Z})$ and some $(u, v) \in R_D$.

To prove this claim, we apply induction on $\Omega(D)$, the number of prime factors of D counted with multiplicity.

If $\Omega(D) = 1$, then $D = p$, a prime congruent to 1 modulo 3. So

$$R_p = \{(u, v) \mid p = u^2 + 3v^2, u > 0, v > 0, (u, 3v) = 1\}.$$

Let $(x, y, z) \in Y^1_D(\mathbb{Z})^*$. Then $xyz \neq 0, x^2 + 3y^2 = 4pz^3, (y, z) = 1$. As we already observed, $p = u^2 + 3v^2$ for unique positive integers u, v such that $(u, 3v) = 1$. Hence, $(u, v) \in R_p$. Further, as we have shown in the proof of Proposition 3.5, p divides exactly one of the integers $uy - vx, uy + vx$.

If $uy \equiv vx \bmod p$, then $uy + vx \not\equiv 0 \bmod p$, and $ux + 3vy \equiv 0 \bmod p$.

If $uy \equiv -vx \bmod p$, then $uy - vx \not\equiv 0 \bmod p$, and $ux - 3vy \equiv 0 \bmod p$.

Thus, if $uy \equiv vx \bmod p$, then $(x_1, y_1, z_1) := (\frac{ux+3vy}{p}, \frac{uy-vx}{p}, z) \in Y^1_1(\mathbb{Z})$ and

$$[p]^-(x_1, y_1, z_1) = (ux_1 - 3vy_1, uy_1 + vx_1, z) = (x, y, z).$$

Similarly, if $uy \equiv -vx \bmod p$, then $(x_1, y_1, z_1) := (\frac{ux-3vy}{p}, \frac{uy+vx}{p}, z) \in Y^1_1(\mathbb{Z})$ and

$$[p]^+(x_1, y_1, z_1) = (ux_1 + 3vy_1, uy_1 - vx_1, z) = (x, y, z).$$

This proves the claim when $\Omega(D) = 1$.

Now, let $\Omega(D) > 1$ and assume that the statement holds for admissible integers A co-prime to 3 for which $\Omega(A) < \Omega(D)$. In other words, we assume for such A that every element of $Y^1_A(\mathbb{Z})^*$ is of the form $(ux_0 \pm 3vy_0, uy_0 \mp vx_0, z_0)$ for some $(x_0, y_0, z_0) \in Y^1_1(\mathbb{Z})$ and some $(u, v) \in R_A$.

Write $D = Aq$ for a prime $q = u_1^2 + 3v_1^2$ congruent to 1 modulo 3. There are two possibilities: either $q \mid A$ or $q \nmid A$.

First, we assume that $q \nmid A$. Now, if $(u, v) \in R_A$, then $u^2 + 3v^2 = A, (u, 3v) = 1, u > 0, v > 0\}$. Then $(|u^+|, |v^-|), (|u^-|, |v^+|) \in R_{Aq}$, where $u^{\pm} = uu_1 \pm 3vv_1, v^{\pm} = vu_1 \mp uv_1$.

Let $(x,y,z) \in Y^1_{Aq}(\mathbb{Z})^*$. Then,

$$[q]_*(x,y,z) = (x_1,y_1,z) \in Y^1_A(\mathbb{Z})^*,$$

where $x_1 = \frac{u_1x \pm 3v_1y}{q}, y_1 = \frac{u_1y \mp v_1x}{q}$ and the signs are such that the entries are integers.

By induction hypothesis, any element of $Y^1_A(\mathbb{Z})^*$ is of the form $(ux_0 \pm 3vy_0, uy_0 \mp vx_0, z_0)$ for some $(x_0,y_0,z_0) \in Y^1_1(\mathbb{Z})$ and some $(u,v) \in R_A$. Therefore $(x_1,y_1,z) = (ux_0 \pm 3vy_0, uy_0 \mp vx_0, z_0)$ for some $(x_0,y_0,z_0) \in Y^1_1(\mathbb{Z})$ and some $(u,v) \in R_A$. Now $[q]^{\mp}(x_1,y_1,z_1) = (x,y,z)$ where the signs are as in $x_1 = \frac{u_1x \pm 3v_1y}{q}, y_1 = \frac{u_1y \mp v_1x}{q}$.

In order to not confuse with the sign appearing in $(x_1,y_1,z) = (ux_0 \pm 3vy_0, uy_0 \mp vx_0, z_0)$, we consider the two cases separately: (i) when $x_1 = \frac{u_1x+3v_1y}{q}, y_1 = \frac{u_1y-v_1x}{q}$, and (ii) when $x_1 = \frac{u_1x-3v_1y}{q}, y_1 = \frac{u_1y+v_1x}{q}$.

In Case (i), we have

$$\begin{aligned} x &= u_1x_1 - 3v_1y_1 = u_1(ux_0 \pm 3vy_0) - 3v_1(uy_0 \mp vx_0) \\ &= (u_1u \pm 3vv_1)x_0 + 3(\pm vu_1 - v_1u)y_0 = u_2x_0 + 3v_2y_0 \end{aligned}$$

where $u_2 = u_1u \pm 3vv_1, v_2 = \pm vu_1 - v_1u$.

Also, in this Case (i), we have

$$\begin{aligned} y &= u_1y_1 + v_1x_1 = u_1(uy_0 \mp vx_0) + v_1(ux_0 \pm 3vy_0) \\ &= (\mp vu_1 + v_1u)x_0 + (u_1u \pm 3vv_1)y_0 = -v_2x_0 + u_2y_0. \end{aligned}$$

As $(x_0,y_0,z) \in Y^1_1(\mathbb{Z})$ implies $(\pm x_0, \pm y_0, z) \in Y^1_1(\mathbb{Z})$, we may take $u_3 = |u_2|$ and $v_3 = |v_2|$ such that $(x,y,z) = (u_3x_0' + v_3y_0', u_3y_0' - v_3x_0', z)$. This proves the claim in Case (i). The Case (ii) is completely analogous.

Finally, we consider the second possibility $q \mid A$; hence $D = Bq^2$ where $q \nmid B$ (as D is cube-free) and B is an admissible integer not divisible by 3.

Write $q = u_1^2 + 3v_1^2$ as before; we have $q^2 = \alpha^2 + 3\beta^2$ where $\alpha = u_1^2 - 3v_1^2, \beta = 2u_1v_1$.

Let $(x,y,z) \in Y^1_{Bq^2}(\mathbb{Z})^*$. So, $x^2 + 3y^2 = 4Bq^2z^3$, and we have then

$$(\alpha y + \beta x)(\alpha y - \beta x) = \alpha^2y^2 - \beta^2x^2 \equiv (\alpha^2 + 3\beta^2) \equiv 0 \mod q^2.$$

So q divides one of $\alpha y \pm \beta x$. If it divides both, then $q \mid y$ which is a contradiction to the fact $(x,y,z) \in Y^1_{Bq^2}(\mathbb{Z})^*$ (as this implies $q \nmid y$ as $q^2 \mid D = Bq^2$). Hence q divides exactly one of $\alpha y \pm \beta x$.

Consider first the case when q divides $\alpha y - \beta x$ and does not divide $\alpha y + \beta x$. Then the fact that q^2 divides $\alpha^2y^2 - \beta^2x^2$ implies that q^2 divides $\alpha y - \beta x$.

Again, the equality $(\alpha x + 3\beta y)^2 + 3(\alpha y - \beta x)^2 = 4Bq^4$ gives that q^2 divides $\alpha x + 3\beta y$.

Observe

$$(x_1, y_1, z) := \left(\frac{\alpha x + 3\beta y}{q^2}, \frac{\alpha y - \beta x}{q^2}, z \right) \in Y_B^1(\mathbb{Z})^*.$$

By induction hypothesis, one can write

$$(x_1, y_1, z) = (ux_0 \pm 3vy_0, uy_0 \mp vx_0, z)$$

where $(x_0, y_0, z) \in Y_1^1(\mathbb{Z})$ and $(u, v) \in R_B$. We have

$$[q]^{--}(x_1, y_1, z) = (\alpha x_1 - 3\beta y_1, \alpha y_1 + \beta x_1, z) = (x, y, z).$$

Putting $(x_1, y_1, z) = (ux_0 \pm 3vy_0, uy_0 \mp vx_0, z)$, we have

$$\begin{aligned}(x, y, z) &= (x_0(\alpha u \pm 3\beta v) + 3y_0(\pm\alpha v - \beta u), y_0(\alpha u \pm 3\beta v) - x_0(\pm\alpha v - \beta u), z) \\ &= u_2 x_0 + 3v_2 y_0, u_2 y_0 - v_2 x_0, z)\end{aligned}$$

where $(u_2 = \alpha u \pm 3\beta v, v_2 = \pm\alpha v - \beta u$. We change the signs of x_0, y_0 to ensure that u_2, v_2 are positive. Note that then $(u_2, v_2) \in R_{Bq^2}$.

The case when q divides $\alpha y + \beta x$ and does not divide $\alpha y - \beta x$ is completely analogous; we will use $[q]^{++}$ in that case.

Hence, the lemma is proved. □

Proposition 3.10. *Let D be an admissible integer with $3 \nmid D$. Suppose $(x_0, y_0, z_0) \in Y_1^1(\mathbb{Z})$ and $(u_j, v_j) \in R_D$ where R_D is as in the lemma above. Then*

$$((u_j x_0 - 3v_j y_0), (u_j y_0 + v_j x_0), z_0) \in Y_D^1(\mathbb{Z})^* \Leftrightarrow (D, z_0, u_j y_0 + v_j x_0) = 1;$$

$$((u_j x_0 + 3v_j y_0), (u_j y_0 - v_j x_0), z_0) \in Y_D^1(\mathbb{Z})^* \Leftrightarrow (D, z_0, u_j y_0 - v_j x_0) = 1.$$

Proof. First, suppose $((u_j x_0 - 3v_j y_0), (u_j y_0 + v_j x_0), z_0) \in Y_D^1(\mathbb{Z})^*$, where $(x_0, y_0, z_0) \in Y_1^1(\mathbb{Z})$. Then, $(u_j y_0 + v_j x_0, z_0) = 1$ which evidently implies $(D, z_0, u_j y_0 + v_j x_0) = 1$. Conversely, suppose $(D, z_0, u_j y_0 + v_j x_0) = 1$. We will show that

$$\begin{aligned}&((u_j x_0 - 3v_j y_0), (u_j y_0 + v_j x_0), z_0) \in Y_D^1(\mathbb{Z})^* \Leftrightarrow \\ &\qquad ((u_j x_0 - 3v_j y_0), (u_j y_0 + v_j x_0), z_0) \in Y_D^1(\mathbb{Z}).\end{aligned}$$

Assume that $((u_j x_0 - 3v_j y_0), (u_j y_0 + v_j x_0), z_0) \in Y_D^1(\mathbb{Z})$ but that $((u_j x_0 - 3v_j y_0), (u_j y_0 + v_j x_0), z_0) \notin Y_D^1(\mathbb{Z})^*$. Then $(u_j y_0 + v_j x_0, z_0) > 1$ while $(D, z_0, u_j y_0 + v_j x_0) = 1$. Let q be a prime dividing $(u_j y_0 + v_j x_0, z_0)$ whereas $q \nmid D$. But, then

$$(u_j x_0 - 3v_j y_0)^2 + 3(u_j y_0 + v_j x_0)^2 = 4Dz_0^3 \Rightarrow q | (u_j x_0 - 3v_j y_0).$$

Hence $q \,|\, (u_j(u_j x_0 - 3v_j y_0) + 3v_j(u_j y_0 + v_j x_0))$; i.e. $q \,|\, Dx_0$. So, $q \,|\, x_0$ and hence $q \,|\, u_j y_0$ as well as $q \,|\, 3v_j y_0$. As $(u_j, 3v_j) = 1$, we get $q \,|\, y_0$. This implies q divides $x_0^2 + 3y_0^2 = 4z_0^3$ and hence $q \,|\, z_0$ which is a contradiction to $(y_0, z_0) = 1$. Therefore,

we have shown that $((u_jx_0 - 3v_jy_0), (u_jy_0 + v_jx_0), z_0) \in Y_D^1(\mathbb{Z})^*$ if and only if $((u_jx_0 - 3v_jy_0), (u_jy_0 + v_jx_0), z_0) \in Y_D^1(\mathbb{Z})$ if and only if $(D, z_0, u_jy_0 + v_jx_0) = 1$.

The other assertion is completely similar. □

4. Irreducible Trinomials Up to Rational Equivalence

First, we describe the sets $X_1^D(\mathbb{Z})^*$. To do this, we essentially keep track of the results proved in Secs. 2 and 3.

Theorem 4.1. *Let $D > 1$ be an admissible integer with $3 \nmid D$. Let $R_D = \{(u_j, v_j) \in \mathbb{Z}^2 \mid D = u_j^2 + 3v_j^2, u_j > 0, v_j > 0, (u_j, 3v_j) = 1\}$ and $r_D = |R_D|$. Then, the set $X_1^D(\mathbb{Z})^* = \bigcup_{j=1}^{r_D} X^{D(j)}$ where $X^{D(j)}$ is given by*

$$\{(9D(u_jy \pm v_jx), D(u_jx \mp 3v_jy), 3Dz) \mid (x, y, z) \in Y_1^1(\mathbb{Z}), (D, z, u_jy \pm v_jx) = 1\}$$
$$\sqcup \left\{(D(u_jx \mp 3v_jy), D\left(\frac{(u_jy \pm v_jx)}{3}\right), Dz) \mid (x, y, z) \in Y_1^1(\mathbb{Z}),\right.$$
$$\left. 3 \mid (u_jy \pm v_jx), (D, z, u_jy \pm v_jx) = 1\right\}.$$

The set $X_1^{9D}(\mathbb{Z})^* = \bigcup_{j=1}^{r_D} X^{D(j)}$ where $X^{D(j)}$ is given by

$$\{(27D(u_jx \mp 3v_jy), 9D(u_jy \pm v_jx), 9Dz) \mid (x, y, z) \in Y_1^1(\mathbb{Z}),$$
$$3 \nmid (u_jy \pm v_jx), (D, z, u_jy \pm v_jx) = 1\}.$$

Proof. Note that from Proposition 3.10, we have $Y_D^1(\mathbb{Z})^* = \bigcup_{j=1}^{r_D} \tilde{Y}_{D(j)}$ where

$$\tilde{Y}_{D(j)} = \{(u_jx \mp 3v_jy, u_jy \pm v_jx, z) \mid (x, y, z) \in Y_1^1(\mathbb{Z}), (D, z, u_jy \pm v_jx) = 1\}.$$

Now statement (2) follows from Corollary 2.7 via the map δ_D.

For the statement (1), we first get $X_D^1(\mathbb{Z})^*$ from $Y_D^1(\mathbb{Z})^*$ by Lemma 2.10. We see that $X_D^1(\mathbb{Z})^* = \bigcup_{j=1}^{r_D} X_{D(j)}$, where $X_{D(j)}$ is given by

$$\{(9(u_jy \pm v_jx), (u_jx \mp 3v_jy), 3z) \mid (x, y, z) \in Y_1^1(\mathbb{Z}), (D, z, u_jy \pm v_jx) = 1\}$$
$$\sqcup \left\{((u_jx \mp 3v_jy), \left(\frac{(u_jy \pm v_jx)}{3}\right), z) \mid (x, y, z) \in Y_1^1(\mathbb{Z}),\right.$$
$$\left. 3 \mid (u_jy \pm v_jx), (D, z, u_jy \pm v_jx) = 1\right\}.$$

Finally, using the map θ_D, we obtain $X_1^D(\mathbb{Z})^* = \bigcup_{j=1}^{r_D} X^{D(j)}$. □

Remark 4.2. We remark that starting from a point $(x_0, y_0, z_0) \in Y_1^1(\mathbb{Z})$ it is not so easy to determine exactly how many points we get in $X_D^1(\mathbb{Z})^*$ using level raising maps (even in the case when $D = p$ a prime).

For instance $(-1,1,1) \in Y_1^1(\mathbb{Z})$ gives three points $(9,-5,3),(27,1,3),(1,1,1) \in X_7^1(\mathbb{Z})$, the point $(37,1,7) \in Y_1^1(\mathbb{Z})$ gives only two points $(351,71,21),(71,13,7) \in X_7^1(\mathbb{Z})$ and the point $(20,18,7) \in Y_1^1(\mathbb{Z})$ gives just one point $(144,94,21) \in X_7^1(\mathbb{Z})$. It is possible to show that if $3 \mid (u \pm v)$, where $p = u^2+3v^2$, then one point in $Y_1^1(\mathbb{Z})$ will give rise to at most three points in $X_p^1(\mathbb{Z})$. On the other hand if $3 \mid v$, that is, if p is a prime expressible as m^2+27n^2, then from a point in $Y_1^1(\mathbb{Z})$ we get either 1 or 2 or 4 points in $X_p^1(\mathbb{Z})$. We remark that for a prime $p \equiv 1 \pmod 3$, the condition $3 \mid v$ is equivalent to 2 being a cubic residue modulo p (see [4, Proposition 9.6.2]).

One can write $X_1^D(\mathbb{Z})^*$ for general admissible D in parametric form and characterize those elements $(x_0,y_0,z_0) \in X_1^D(\mathbb{Z})^*$ for which the trinomial $X^3 - z_0X + y_0$ is irreducible. Towards that, we observe

Lemma 4.3. *Let $f(X) = X^3 - aX + b \in \mathbb{Z}[X]$ be a cubic polynomial whose discriminant is a perfect square. If $(a,b) = d > 1$ is cube-free and for each prime l such that $l^2|d$, we have $l^3 \nmid b$, then $f(X)$ is irreducible.*

Proof. If $d > 1$ is square-free, then for any prime divisor l of d, we have $l^2 \nmid b$. If not, then this implies $l \,||\, a$ and $l^2 \mid b$. Hence, $l^3 \mid 4a^3 - 27b^2 = c^2$ and hence $l^2 \mid c$, which implies $l^4 \mid c^2 + 27b^2 = 4a^3$, which implies $l^2 \mid a$, contradiction. Thus $f(X)$ satisfies Eisenstein criterion for the prime l and hence irreducible.

If $l^2|d$ for some prime l, then $a = l^2A, b = l^2B$ with $(l,B) = 1$. If

$$X^3 - aX + b = X^3 - l^2Ax + l^2B = (X+r)(X^2+sX+t),$$

then $rt = l^2B$, $s = -r$ and $r^2 - t = l^2A$. Now l divides r or t; if it divides only one of them, we have a contradiction from $r^2 - t = l^2A$. Hence $l|r, l|t$. So, $t = r^2 - l^2A \equiv 0 \mod l^2$. But $rt = l^2B$ with $(l,B) = 1$ implies $l^2 \nmid t$ which is a contradiction. Therefore, $X^3 - aX + b$ is irreducible. □

Theorem 4.4. *For an admissible integer $D > 1$, the irreducible trinomials (up to rational equivalence) of the form $X^3 - aX + b$ with $(a,b) = D$ and discriminant perfect square are given by $X^3 - zX + y$, where y and z are integers such that $(x,y,z) \in X_1^D(\mathbb{Z})^*$. Note that discriminant of the polynomial $X^3 - zX + y$ is x^2.*

Proof. For $(x,y,z) \in X_1^D(\mathbb{Z})^*$, $X^3 - zX + y \in \mathbb{Z}[X]$ has discriminant perfect square and $(y,z) = D$. On the other hand, suppose $X^3 - aX + b$ has discriminant $c^2 = 4a^3 - 27b^2$ and $(a,b) = D$. Thus $(c,b,a) \in X_1^D(\mathbb{Z})$. Since we are considering polynomials up to rational equivalence, we may assume that if for any prime ℓ, $\ell^2 \mid a$ then $\ell^3 \nmid b$. This is equivalent to $(c,b,a) \in X_1^D(\mathbb{Z})^*$.

Since $D > 1$, irreducibility of $X^3 - zX + y$ follows from Lemma 4.3. □

Remark 4.5. (i) When $(a,b) = 1$, the above theorem is not valid as some of the trinomials coming from $X_1^1(\mathbb{Z})$ are reducible. The irreducible ones are determined in the main theorem below.

(ii) We do not claim that these polynomials are rationally inequivalent. In fact the four points $(\pm x, \pm y, z) \in X^D(\mathbb{Z})^*$ generate only one trinomial up to rational equivalence; so even though we have listed all the trinomials, we have listed each multiple times — once for each occurrence of a point in $X^D(\mathbb{Z})^*$.

Using the parametrization of $Y_1^1(\mathbb{Z})$ and combining Theorems 2.9, 2.11, 4.1 and 4.4, we may now write down all irreducible trinomials $X^3 - aX + b \in \mathbb{Z}[X]$ whose discriminant is a perfect square (up to rational equivalence)

Theorem 4.6. *Up to rational equivalence, any irreducible trinomial whose discriminant is a perfect square is* $X^3 - aX + b$ *where* $gcd(a, b)$ *must be* D *or* $9D$*, where* $3 \nmid D$ *and each prime divisor of* D *is congruent to* 1 *modulo* 3*. To describe all of them, write* $D = u_j^2 + 3v_j^2$ *with* $u_j, v_j > 0$ *and* $(u_j, 3v_j) = 1$*,* $j \in \{1, \ldots, r_D\}$*. Let* s *and* t *be co-prime integers with* $3 \nmid (s+t)$*. Up to rational equivalence, the irreducible trinomials of the form* $X^3 - aX + b \in \mathbb{Z}[X]$ *whose discriminant is a perfect square are given as follows*:

(i) *Polynomials with* $(a, b) = 1$ *are given by*

$$f_{(s,t)}(X) = X^3 - 3(s^2 - st + t^2)X \pm ((s+t)^3 - 9st^2).$$

(ii) *Polynomials with* $(a, b) = 9$ *are given by*

$$h_{(s,t)}(X) = X^3 - 9(s^2 - st + t^2)X + 9(s^3 - 3s^2t + t^3).$$

(iii) *Polynomials with* $(a, b) = D$ *are given by*

(a) $f_{D,j,\pm,s,t,1}(X) = X^3 - aX + b$ *where*

$$a = 3D(s^2 - st + t^2), \quad b = D(u_j(s+t)(s-2t)(2s-t) \mp 9v_j st(s-t))$$

if $(D, s^2 - st + t^2, 3u_j st(s-t) \pm v_j(s+t)(s-2t)(2s-t)) = 1$.

(b) $f_{D,j,\pm,s,t,2}(X) = X^3 - aX + b$ *where*

$$a = 3D(s^2 - st + t^2), \quad b = D(u_j((s+t)^3 - 9st^2) \mp 3v_j(s^3 - 3s^2t + t^3))$$

if $(D, s^2 - st + t^2, u_j(s^3 - 3s^2t + t^3) \pm v_j((s+t)^3 - 9st^2)) = 1$.

(c) $g_{D,j,\pm,s,t,1}(X) = X^3 - aX + b$ *where*

$$a = D(s^2 - st + t^2), \quad b = D\left(u_j st(s-t) \pm \frac{v_j}{3}(s+t)(s-2t)(2s-t)\right)$$

if $3 \mid v_j$*, and* $(D, s^2 - st + t^2, 3u_j st(s-t) \pm v_j(s+t)(s-2t)(2s-t)) = 1$.

(d) $g_{D,j,\pm,s,t,2}(X) = X^3 - aX + b$*, where*

$$a = D(s^2 - st + t^2), \quad b = \frac{D}{3}(u_j(s^3 + t^3 - 3s^2t) \pm v_j((s+t)^3 - 9st^2))$$

if $3 \nmid v_j$ (*which means* $3 \mid u_j \pm v_j$) *and* $\big(D, s^2-st+t^2, u_j(s^3+t^3-3s^2t) \pm v_j((s+t)^3-9st^2)\big) = 1$. *We choose* $+$ (*respectively*, $-$) *sign if and only if* $3 \mid u_j + v_j$ (*respectively*, $3 \mid u_j - v_j$).

(iv) *Polynomials with* $(a,b) = 9D$ *are given by*

(a) $h_{9D,j,\pm,s,t,1}(X) = X^3 - aX + b$, *where*

$$a = 9D(s^2-st+t^2), \quad b = 9D(3u_jst(s-t) \pm v_j(s+t)(2s-t)(s-2t))$$

if $3 \nmid v_j$, *and* $(D, s^2-st+t^2, 3u_jst(s-t) \pm v_j(s+t)(2s-t)(s-2t)) = 1$.

(b) $h_{9D,j,\pm,s,t,2}(X) = X^3 - aX + b$, *where*

$$a = 9D(s^2-st+t^2), \quad b = 9D(u_j(s^3-3s^2t+t^3) \pm v_j((s+t)^3-9st^2))$$

if $3 \nmid (u_j \pm v_j)$, *and* $(D, s^2-st+t^2, u_j(s^3-3s^2t+t^3) \pm v_j((s+t)^3-9st^2)) = 1$.

Proof. The theorem is a consequence of Theorems 2.11, 2.9 and 4.4 as we explicitly write down points $(x,y,z) \in X^D(\mathbb{Z})^*$ using the parametrization of $Y_1^1(\mathbb{Z})$ as given in Theorem 2.8 ([1, Proposition 14.2.1(2)]) and Theorem 4.1.

(i) If $(a,b) = 1$, then from Theorem 2.11, we see the corresponding trinomials are $X^3-(s^2-st+t^2)X+st(s-t)$, $X^3-3(s^2-st+t^2)X+(s+t)(2s-t)(s-2t)$ and $X^3-3(s^2-st+t^2)X \pm ((s+t)^3-9st^2)$. Note that $X^3-(s^2-st+t^2)X+st(s-t)$ has a root t and hence is never irreducible. Also, $X^3-3(s^2-st+t^2)X+(s+t)(2s-t)(s-2t)$ has a root $(s+t)$ and hence is never irreducible.

Note that $(s+t)^3 - 9st^2$ and $st(s-t)$ are always odd (as both s and t cannot be even), hence

$$X^3 - 3st(s-t)X \pm ((s+t)^3 - 9st^2) \equiv X^3 + X + 1 \pmod 2,$$

as a consequence we see that $X^3 - 3st(s-t)X + (s+t)^3 - 9st^2$ is irreducible.

(ii) The polynomials are obtained from Theorem 2.9. The statement regarding irreducible polynomials follows from Theorem 4.4.

(iii) Combining the parametrization of $Y_1^1(\mathbb{Z})$ as given in [1, Proposition 14.2.1(2)] and Theorem 4.1 we get $X_1^D(\mathbb{Z})^* = \cup_{j=1}^{r_D} X^{D(j)}$, where $X^{D(j)}$ is the set given explicitly as

$$\begin{aligned}
&\{(9D(3u_jst(s-t) \pm v_j(s+t)(s-2t)(2s-t)),\\
&\quad D(u_j(s+t)(s-2t)(2s-t) \mp 9v_jst(s-t)), 3D(s^2-st+t^2))|\\
&\quad (D, s^2-st+t^2, 3u_jst(s-t) \pm v_j(s+t)(s-2t)(2s-t)) = 1\}\\
&\cup \{(\pm 9D(u_j(s^3-3s^2t+t^3) \pm v_j((s+t)^3-9st^2)),\\
&\quad \pm D(u_j((s+t)^3-9st^2) \mp 3v_j(s^3-3s^2t+t^3)), 3D(s^2-st+t^2))|\\
&\quad (D, s^2-st+t^2, u_j(s^3-3s^2t+t^3) \pm v_j((s+t)^3-9st^2)) = 1\}\\
&\cup \{(D(u_j(s+t)(s-2t)(2s-t) \mp 9v_jst(s-t)),
\end{aligned}$$

$$D(u_jst(s-t)\pm\frac{v_j}{3}(s+t)(s-2t)(2s-t)), D(s^2-st+t^2))|$$
$$3\mid v_j, (D, s^2-st+t^2, 3u_jst(s-t)\pm v_j(s+t)(s-2t)(2s-t))=1\}$$
$$\cup\{\pm(D(u_j((s+t)^3-9st^2)\mp 3v_j(s^3+t^3-3s^2t)),$$
$$\pm\frac{D}{3}(u_j(s^3+t^3-3s^2t)\pm v_j((s+t)^3-9st^2)),$$
$$D(s^2-st+t^2))|3|u_j\pm v_j, (D, s^2-st+t^2, u_j(s^3+t^3-3s^2t)$$
$$\pm v_j((s+t)^3-9st^2))=1\}.$$

We remark that

$$3\mid 3u_jst(s-t)\pm v_j(s+t)(s-2t)(2s-t)\Leftrightarrow 3\mid v_j$$

and

$$3\mid u_j(s^3+t^3-3s^2t)\pm v_j((s+t)^3-9st^2)\Leftrightarrow 3\mid (u_j\pm v_j).$$

Since $(u_j, 3v_j)=1$, we get $3\mid (u_j\pm v_j)$ if and only if $3\nmid v_j$.

Also note that the points $(\pm x, \pm y, z)\in X_1^D(\mathbb{Z})^*$ give rise to only one trinomial up to rational equivalence; we only consider the expressions for x, y, z while writing down the polynomials $f_{D,j,\pm,s,t,2}(X)$ and $g_{D,j,\pm,s,t,2}(X)$. The statement regarding irreducibility of the trinomials follows from Theorem 4.4.

(iv) Combining the parametrization of $Y_1^1(\mathbb{Z})$ as given in [1, Proposition 14.2.1(2)] and Theorem 4.1 we get $X_1^{9D}(\mathbb{Z})^*=\cup_{j=1}^{r_D}X^{9D(j)}$, where $X^{9D(j)}$ is the set

$$\{(27D(u_j(s+t)(2s-t)(s-2t)\mp 9v_jst(s-t)),$$
$$9D(3u_jst(s-t)\pm v_j(s+t)(2s-t)(s-2t)), 9D(s^2-st+t^2))\mid 3\nmid v_j$$
$$(D, s^2-st+t^2, 3u_jst(s-t)\pm v_j(s+t)(2s-t)(s-2t))=1\}$$
$$\cup\{(\pm 27D(u_j((s+t)^3-9st^2)\mp 3v_j(s^3-3s^2t+t^3)),$$
$$\pm 9D(u_j(s^3-3s^2t+t^3)\pm v_j((s+t)^3-9st^2)),$$
$$9D(s^2-st+t^2))\mid 3\nmid (u_j\pm v_j),$$
$$\big(D, s^2-st+t^2, u_j(s^3-3s^2t+t^3)\pm v_j((s+t)^3-9st^2))=1\}.$$

We remark that

$$3\nmid (3u_jst(s-t)\pm v_j(s+t)(2s-t)(s-2t))\Leftrightarrow 3\nmid v_j$$

and

$$3\nmid (u_j(s^3-3s^2t+t^3)\pm v_j((s+t)^3-9st^2))\Leftrightarrow 3\nmid (u_j\pm v_j).$$

Also note that the points $(\pm x, \pm y, z)\in X_1^{9D}(\mathbb{Z})^*$ give rise to only one trinomial up to rational equivalence; we only consider the expressions for x, y, z while writing down the polynomials $h_{D,j,\pm,s,t,2}(X)$. The statement regarding irreducible trinomials follows from Theorem 4.4. □

5. Cube-Free Natural Numbers Expressible as Sums of Two Rational Cubes

As an accidental byproduct of our results above, we can partially solve a classical problem. A classical, open problem (see [9]) in number theory asks for a classification of all cube-free natural numbers which can be expressed as sums of cubes of two rational numbers.

We give an alternate description of these numbers in terms of non-trivial integral points of $X_1(\mathbb{Z})$. Let n be a cube-free natural number. Observe that the affine curve $x^3+y^3=n$ is isomorphic to the affine curve $X^2=4Z^3-27n^2$ given by the following change of variables:

$$x=\frac{9n+X}{6Z} \quad \text{and} \quad y=\frac{9n-X}{6Z}, \tag{2}$$

and

$$X=\frac{3n}{x+y} \quad \text{and} \quad Y=9n\frac{x-y}{x+y}. \tag{3}$$

Let us denote by E_n the elliptic curve whose Weierstrass equation is given by $Y^2=4X^3-27n^2$. (We remark that the elliptic curve E_n is isomorphic to E_{nm^3} over $\mathbb{Q}$.) Then, we can identify (the projectivization of) $x^3+y^3=n$ with the elliptic curve E_n. As a consequence, we see that n can be written as sum of two rational cubes if and only if $E_n(\mathbb{Q})$ is non-trivial. It is well known (see [2]) that $E_n(\mathbb{Q})_{\text{tors}}=\{\mathcal{O}\}$ if $n>2$. Thus, a cube-free natural number $n>2$ is can be expressed as a sum of two rational cubes if and only if $\text{rk}(E_n(\mathbb{Q}))>0$. The standard approach to study this problem is via the theory of (mock) Heegner points. But, in what follows, we relate this to the integral solutions of the equation $X^2+27Y^2=4Z^3$.

Definition 5.1. Let S denote the set of cube-free natural numbers given by

$$S=\{n \mid n>2, (a,nm^3,b)\in X_1^D(\mathbb{Z})^* \text{ for some } a,b,m\in\mathbb{Z} \text{ and for some admissible } D\}.$$

Theorem 5.2. *Let $n>2$ be a cube-free natural number. Then n is a sum of cubes of two rational numbers if and only if $n\in S$, where S is as defined above.*

Proof. Let $n\in S$. Then there exist integers a,b,m such that $(a,nm^3,b)\in X_1^{non-triv}(\mathbb{Z})$ - or, equivalently - (a,b) satisfies the equation $X^2=4Z^3-27(nm^3)^2$. Then from (2), it follows that $\left(\frac{9nm^3+a}{6b},\frac{9nm^3-a}{6b}\right)$ satisfies the equation $x^3+y^3=nm^3$. As a consequence, we have

$$n=\left(\frac{9nm^3+a}{6bm}\right)^3+\left(\frac{9nm^3-a}{6bm}\right)^3.$$

Conversely, let n be a cube-free natural number and suppose $q_1 = \frac{a_1}{db_1}$ and $q_2 = \frac{a_2}{db_2}$ (with $(a_1, db_1) = (a_2, db_2) = (b_1, b_2) = 1$) are two rational numbers such that $q_1^3 + q_2^3 = n$. Then

$$(a_1b_2)^3 + (a_2b_1)^3 = nd^3b_1^3b_2^3.$$

If $\ell \mid b_1$, then $\ell^3 \mid b_1^3$, which implies $\ell^3 \mid (nd^3b_2^3 - a_2^3)b_1^3 = (a_1b_2)^3$ or equivalently $\ell \mid a_1b_2$. This is impossible as $(a_1, b_1) = (b_1, b_2) = 1$. A similar argument shows that $\ell \mid b_2$ is also impossible. We conclude that $b_1b_2 = \pm 1$. If necessary, changing the signs of a_1 and a_2, we may assume that $b_1 = b_2 = 1$.

Since $\left(\frac{a_1}{d}, \frac{a_2}{d}\right)$ satisfies $x^3 + y^3 = n$, from (3), we see that $\left(9n\frac{a_1 - a_2}{a_1 + a_2}, \frac{3nd}{a_1 + a_2}\right)$ (note that $a_1 + a_2 \neq 0$) satisfies $X^2 = 4Z^3 - 27n^2$. Hence

$$\left(9n\frac{a_1 - a_2}{a_1 + a_2}, n, \frac{3nd}{a_1 + a_2}\right) \in X_1(\mathbb{Q}).$$

As a consequence, we see that $\left(9n\frac{a_1-a_2}{a_1+a_2}m^3, nm^3, \frac{3nd}{a_1+a_2}m^2\right) \in X_1(\mathbb{Q})$, for any natural number m. Since $a_1^3 + a_2^3 = nd^3$, it follows that $(a_1 + a_2) \mid nd^3$. Taking $m = d$, we obtain

$$\left(9(a_1 - a_2)\frac{nd^3}{a_1 + a_2}, nd^3, 3\frac{nd^3}{a_1 + a_2}\right) \in X_1(\mathbb{Z}).$$

Now note that $a_1 \neq a_2$ as $n \neq 2$. Thus $(9(a_1 - a_2)\frac{nd^3}{a_1+a_2}, nd^3, 3\frac{nd^3}{a_1+a_2}) \in X_1^{non-triv}(\mathbb{Z})$, here $X_1^{non-triv}(\mathbb{Z}) = \{(x, y, z) \in \mathbb{Z}^3 \mid x^2 + 27y^2 = 4z^3, xyz \neq 0\}$, which are the complements of the trivial integrals zeros $X_1^{\text{triv}}(\mathbb{Z})$. Observe that if $(x, y, z) \in X_1^{non-triv}(\mathbb{Z})$ and $\ell^3 \mid y$ and $\ell^2 \mid z$, then $\ell^3 \mid x$ and $\left(\frac{x}{\ell^3}, \frac{y}{\ell^3}, \frac{z}{\ell^2}\right) \in X_1^{non-triv}(\mathbb{Z})$. As a consequence we see that if $\ell \mid d$ is a prime such that $\ell^2 \mid 3\frac{nd^3}{a_1+a_2}$, then $\ell^3 \mid 9(a_1 - a_2)\frac{nd^3}{(a_1+a_2)}$ and hence $(9(a_1 - a_2)\frac{nd^3}{\ell^3(a_1+a_2)}, \frac{nd^3}{\ell^3}, 3\frac{nd^3}{\ell^2(a_1+a_2)}) \in X_1^{non-triv}(\mathbb{Z})$. Proceeding in this manner, we see that there exists a largest natural number k such that $k \mid d$ and

$$\left(9(a_1 - a_2)\frac{nd^3}{k^3(a_1 + a_2)}, \frac{nd^3}{k^3}, 3\frac{nd^3}{k^2(a_1 + a_2)}\right) := (a, nm^3, b) \in X_1^{non-triv}(\mathbb{Z}).$$

Note that $(a, nm^3, b) \in X_1^D(\mathbb{Z})$ for $D = gcd(nm^3, b)$. If for a prime ℓ, $\ell^3 \mid D$, then we see that $(9(a_1 - a_2)\frac{nd^3}{(k\ell)^3(a_1+a_2)}, \frac{nd^3}{(k\ell)^3}, 3\frac{nd^3}{(k\ell)^2(a_1+a_2)}) \in X_1^{non-triv}(\mathbb{Z})$, which contradicts the maximality of k. Hence D is cube-free.

Similarly, if $\ell^3 \mid nm^3$ and $\ell^2 \mid b$, then again $(9(a_1 - a_2)\frac{nd^3}{(k\ell)^3(a_1+a_2)}, \frac{nd^3}{(k\ell)^3}, 3\frac{nd^3}{(k\ell)^2(a_1+a_2)}) \in X_1^{non-triv}(\mathbb{Z})$, which contradicts the maximality of k. Thus $(a, nm^3, b) \in X_1^D(\mathbb{Z})^*$ for an admissible D. □

In order to deduce that certain primes are expressible as sums of two rational cubes, we recall that $(9(s^3 - 3s^2t + t^3), (s + t)^3 - 9st^2, 3(s^2 - st + t^2)) \in X_1^1(\mathbb{Z})$ for any co-prime integers s, t with $3 \nmid (s + t)$. As a consequence, we obtain

Corollary 5.3. *Let $p \equiv \pm 1 \pmod 9$ be a prime and m be an integer such that $pm^3 = (s+t)^3 - 9st^2$ for some co-prime integers s and t. Then p can be written as*

a sum of two rational cubes. Explicitly

$$p = \left(\frac{s^3+t^3-3st^2}{m(s^2-st+t^2)}\right)^3 + \left(\frac{3st(s-t)}{m(s^2-st+t^2)}\right)^3.$$

Remark 5.4. There are infinitely many primes which satisfy the hypotheses of corollary 5.3; see [3, Theorem 1.1]. By work of Stagé [8], we know that odd primes p which are congruent to $2, 5$ modulo 9 cannot be expressed as a sum of two rational cubes. Recent work of Dasgupta and Voight [2] shows that primes p congruent to 4 or 7 modulo 9 can be expressed as a sum of rational cubes if 3 is not a cubic residue modulo p. Rodriguez-Villegas and Zagier [6] - assuming the truth of the BSD conjecture - give a criterion to decide whether a prime 1 modulo 9 can be expressed as a sum of two rational cubes. The authors do not know of any previous unconditional result describing when primes congruent to ± 1 modulo 9 are expressible as sums of two rational cubes.

Remark 5.5. There are 49 primes less than 2000 which are congruent to 1 modulo 9 and, by the result of [6], we expect that 22 of them are expressible as sums of two rational cubes. If we vary $(s,t,m) \in \mathbb{Z}^3$ with $0 < |s|, |t|, m < 1000$, $(s,t) = 1$, then all of these 22 primes satisfy $pm^3 = (s+t)^3 - 9st^2$ for some choice of (s,t,m). There are 14 primes less than 500 which are congruent to -1 modulo 9 and all of these 14 primes satisfy $pm^3 = (s+t)^3 - 9st^2$ for some choice of (s,t,m) with $(s,t,m) \in \mathbb{Z}^3$ with $0 < |s|, |t|, m < 1000$. There are 50 primes less than 2000 which are congruent to -1 modulo 9, at least 34 out of these 50 primes satisfy $pm^3 = (s+t)^3 - 9st^2$ for some choice of (s,t,m). All of these were verified using Sage [7].

From the above data, we may hazard a guess that there are infinitely many primes congruent to 1 (respectively, -1) modulo 9 which satisfy the condition of Corollary 5.3.

Further, one can verify that if a tuple $(a, nm^3, b) \in X_1^D(\mathbb{Z})^*$, then $(D,m) = 1$. Since elements of $X_1^D(\mathbb{Z})^*$ are of the form (Dx, Dy, Dz), it follows that $D \mid nm^3$ and hence $D \mid n$. Now, for a prime p which is congruent to -1 modulo 9, if $(a, nm^3, b) \in X_1^D(\mathbb{Z})^*$ then it follows that $D = 1$, as $X_1^p(\mathbb{Z})^* = \emptyset$. As a consequence $p \equiv -1 \pmod 9$ can be written as sum of two rational cubes if and only if there exists integers s, t, m with $(s,t) = 1$ for which at least one of the following condition holds:

(1) $pm^3 = (s+t)^3 - 9st^2$,
(2) $pm^3 = st(s-t)$.

Note that as $(s+t)(2s-t)(s-2t) = 2(s+t)^3 - 9st(s+t) \equiv \pm 2 \pmod 9$, we did not include it in the list. We could not find any tuple $(s,t,m) \in \mathbb{Z}^3$ such that $pm^3 = st(s-t)$. This leads us to believe that $p \equiv -1 \pmod 9$ is expressible as sum of rational cubes if and only if it satisfies the condition of Corollary 5.3.

Acknowledgments

It is a pleasure to thank the referee for her/his suggestions which helped us improve the presentation of the results. The referee's detailed comments also helped us in correcting some minor errors and the language also at various places. We are indebted to the referee for also pointing out the primes 883 and 937 which correspond to the triples $(s,t,m) = (14,195,17)$ and $(s,t,m) = (8,203,19)$ in Remark 5.5. Finally, we also thank S. Panda and P. Shingavekar for pointing out that the primes 701 and 1151 which correspond to $(77,1299,127)$ and $(1137,-250,37)$, respectively.

References

[1] H. Cohen, *Number Theory, Volume II: Analytic and Modern Tools*, Graduate Text in Mathematics, Vol. 240 (Springer-Verlag, 2007).
[2] S. Dasgupta and J. Voight, Sylvester's problem and mock Heegner points, *Proc. Amer. Math. Soc.* **146** (2018) 3257–3273.
[3] D. R. Heath-Brown and B. Z. Moroz, Primes represented by binary cubic forms, *Proc. London Math. Soc.* (*3*) **84**(2) (2002) 257–288.
[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Text in Mathematics, Vol. 84, 2nd edition (Springer-Verlag, 1990).
[5] P. Morandi, *Field and Galois Theory*, Graduate Text in Mathematics, Vol. 167, 1st edition (Springer-Verlag, 1997).
[6] F. Rodriguez-Villegas and D. Zagier, Which primes are sum of two cubes? *Number Theory* (Halifax, NS, 1994), *CMS Conf. Proc.*, Vol. 15 (American Mathematical Society, Providence, 1995), pp. 521–532.
[7] Sage Mathematics Software, http://www.sagemath.org.
[8] P. Stagé, Groupes de Selmer et corps cubiques, *J. Number Theory* **23** (1986) 294–317.
[9] E. S. Selmer, The diophantine equation $ax^3 + by^3 + cz^3 = 0$, *Acta Math.* **85** (1951) 203–362.