ON THE SUMS OF TWO CUBES

BRUCE REZNICK AND JEREMY ROUSE

ABSTRACT. We solve the equation $f(x,y)^3 + g(x,y)^3 = x^3 + y^3$ for homogeneous $f, g \in \mathbb{C}(x,y)$, completing an investigation begun by Viète in 1591. The usual addition law for elliptic curves and composition give rise to two binary operations on the set of solutions. We show that a particular subset of the set of solutions is ring-isomorphic to $\mathbb{Z}[e^{2\pi i/3}]$.

1. INTRODUCTION

In 1591, François Viète published a revolutionary work on algebra which has been translated into English [10] as *The Analytic Art*. Viète's "Zetetic XVIII" [10, p.145] is:

> Given two cubes, to find numerically two other cubes the sum of which is equal to the difference between those that are given.

> Let the two given cubes be B^3 and D^3, the first the greater, the second the smaller. Two other cubes are to be found, the sum of which is equal to $B^3 - D^3$. Let $B - A$ be the root of the first one that is to be found, and let $B^2A/D^2 - D$ be the root of the second. Forming the cubes and comparing them with $B^3 - D^3$, it will be found that $3D^3B/(B^3 + D^3)$ equals A. The root of the first cube to be found, therefore, is $[B(B^3 - 2D^3)]/(B^3 + D^3)$ and of the second is $[D(2B^3 - D^3)]/(B^3 + D^3)$. And the sum of the cubes of these is equal to $B^3 - D^3$ .... [So it is if] B is 2 and D 1: The cube of the root 6 will equal the individual cubes of 3, 4 and 5. When, therefore, the cubes of $6x$ and $3x$ are given, the cubes of $4x$ and $5x$ will appear and the sum of the latter will be equal to the difference between the former.

Viète worked at the dawn of algebra, when mathematicians were not yet comfortable with negative numbers; his work can be put into somewhat more modern terminology by setting $B = x$ and $D = -y$. Viète's formula then becomes:

$$(1.1) \qquad x^3 + y^3 = \left(\frac{x(x^3 + 2y^3)}{x^3 - y^3} \right)^3 + \left(\frac{y(y^3 + 2x^3)}{y^3 - x^3} \right)^3 .$$

Equation (1.1) is well-known in number theory; its iteration shows that any sum of two cubes over $\mathbb{Q}$ (except those of the form d^3 and $2d^3$) has infinitely many such representations. See for example [5, §13.7, 21.11]. Continuing Viète's example,

$$(1.2) \qquad 189 = 6^3 + (-3)^3 = 4^3 + 5^3 = \left(-\tfrac{1256}{61}\right)^3 + \left(\tfrac{1265}{61}\right)^3 = \cdots$$

In this paper, we find all solutions to

$$(1.3) \qquad f^3(x,y) + g^3(x,y) = x^3 + y^3,$$

where $f(x,y)$ and $g(x,y)$ are homogeneous rational functions over $\mathbb{C}$. Upon finding a common denominator for (f,g), the equation in (1.3) becomes

$$(1.4) \qquad p^3(x,y) + q^3(x,y) = (x^3 + y^3)r^3(x,y),$$

where $p, q, r \in \mathbb{C}[x,y]$ are homogeneous polynomials (*forms*), $f = p/r$ and $g = q/r$. The degree of the solution is defined to be $\deg(p) = \deg(q) = 1 + \deg(r)$.

In projective terms,

$$(1.5) \qquad (f : g : 1) = (p : q : r).$$

Our principal definition is the following: let

$$(1.6) \qquad \mathcal{V} = \{v = (p : q : r) : \text{where } p, q, r \in \mathbb{C}[x,y] \text{ are forms and satisfy (1.4)}\}.$$

A solution to (1.6) with $r \neq 0$ is projectively equivalent to $(p/r : q/r : 1)$ and we will denote solutions of this type by $(p/r, q/r)$ or (f,g). However, there are three solutions to (1.4) "at infinity" with $r = 0$, namely $(1 : -1 : 0)$, $(1 : -\omega : 0)$, and $(1 : -\omega^2 : 0)$, where

$$(1.7) \qquad \omega := \mathrm{Exp}\left(\tfrac{2\pi i}{3}\right) = -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i.$$

We observe that if π is irreducible and $\pi | p, q$ in (1.4), then $\pi^3 | (x^3 + y^3)r^3$, hence, $\pi^2 | r^3$ (at least), so $\pi | r$. Similarly, if $\pi | p, r$, then $\pi | q$ and if $\pi | q, r$, then $\pi | p$. Since r is a common denominator, no two of $\{p, q, r\}$ have a common factor.

One would ordinarily say that, if $x^3 + y^3 = f_1^3 + g_1^3 = f_2^3 + g_2^3$ and $\{f_1^3, g_1^3\} = \{f_2^3, g_2^3\}$, then (f_1, g_1) and (f_2, g_2) are the same solution; however as "points" on (1.3), each solution occurs 18-fold : as $(\omega^j f, \omega^k g)$ and $(\omega^k g, \omega^j f)$, where $j, k \in \{0, 1, 2\}$. We shall call these elements of $\mathcal{V}$ the *affiliates* of (f,g).

We now list $v = (p : q : r) \in \mathcal{V}$ (up to affiliation) with degree ≤ 12, with the convention that subscripts given below to p, q, r will be inherited by $f = p/r, g = q/r$, and v. (That these are the only such elements will follow from Theorem 1.1.)

Let

$$(1.8) \qquad \zeta := \zeta_{12} = \mathrm{Exp}\left(\tfrac{\pi i}{6}\right) = \tfrac{\sqrt{3}}{2} + \tfrac{i}{2},$$

so that $\zeta + \zeta^{-1} = \sqrt{3}$ and $\zeta^3 + \zeta^{-3} = 0$. We note that there are two solutions of degree 7, the second of which is the complex conjugate of v_7 in the table below.

Degree	Solution
1	$p_1 = x$
	$q_1 = y$
	$r_1 = 1$
3	$p_3 = \zeta^{-1}x^3 + \zeta y^3$
	$q_3 = \zeta x^3 + \zeta^{-1}y^3$
	$r_3 = \sqrt{3}xy$
4	$p_4 = x(x^3 + 2y^3)$
	$q_4 = -y(y^3 + 2x^3)$
	$r_4 = x^3 - y^3$
7	$p_7 = x\left(x^6 + (1 + 3\omega)(x^3y^3 + y^6)\right)$
	$q_7 = y\left((1 + 3\omega)(x^6 + x^3y^3) + y^6\right)$
	$r_7 = x^6 + (1 - 3\omega)x^3y^3 + y^6$
9	$p_9 = -x^9 + 3x^6y^3 + 6x^3y^6 + y^9$
	$q_9 = x^9 + 6x^6y^3 + 3x^3y^6 - y^9$
	$r_9 = 3xy(x^6 + x^3y^3 + y^6)$
12	$p_{12} = -3(x^3 - y^3)^3(x^3 + y^3) - (1 + 2\omega)(x^3(x^3 + 2y^3)^3 + y^3(y^3 + 2x^3)^3)$
	$q_{12} = -3(x^3 - y^3)^3(x^3 + y^3) - (1 + 2\omega^2)(x^3(x^3 + 2y^3)^3 + y^3(y^3 + 2x^3)^3)$
	$r_{12} = 6xy(x^3 - y^3)(2x^3 + y^3)(x^3 + 2y^3)$

Observe that

$$(1.9) \qquad \frac{\zeta}{\sqrt{3}} = \frac{2 + \omega}{3}, \qquad \frac{\zeta^{-1}}{\sqrt{3}} = \frac{2 + \omega^2}{3}$$

so that $f_3, g_3 \in \mathbb{Q}[\omega](x, y)$; see Theorem 1.2(3) below. By setting $x = 6$ and $y = -3$ in v_9, we obtain the rational solution $189 = \left(\frac{219}{38}\right)^3 + \left(\frac{-51}{38}\right)^3$ to (1.2).

We remark that v_4 appears in [3, pp.550-1]. In 1877, Lucas (see [3, p.574]) proved a formula equivalent to v_9; namely, if $x^3 + y^3 = Az^3$, then $q_9^3(x, y) + p_9^3(x, y) = Az^3r_9^3(x, y)$. In 1878, Lucas (see [3, p.575]) gave the identity

$$(1.10) \qquad \begin{aligned} (-x^3 + 3x^2y + 6xy^2 + y^3)^3 + (x^3 + 6x^2y + 3xy^2 - y^3)^3 = \\ 3^3xy(x + y)(x^2 + xy + y^2)^3, \end{aligned}$$

which Desboves later observed (see [3, p.575]) is equivalent to Lucas' previous identity upon taking $(x, y) \mapsto (x^3, y^3)$.

Even though v_3 is not real, its components become real under any map $(x, y) \mapsto (\alpha x + \beta y, \bar{\alpha} x + \bar{\beta} y)$. This map is invertible provided $\alpha\bar{\beta}$ is not real. Taking $(\alpha, \beta) = (\zeta^{-1}, \zeta^1)$ in the expression $f_3^3(x, y) + g_3^3(x, y) = (x^3 + y^3)r_3^3(x, y)$ yields (1.10). Thus, it can be argued that the first "new" solution to (1.3) in the table is v_7. The previous interest in (1.3) required solutions over $\mathbb{Q}$. We shall show in Theorem 1.2(7) that rational solutions only occur for square degree. Since the solution of degree 16 arises from iterating v_4, our first truly new solution over $\mathbb{Q}$ has degree 25.

The set $\mathcal{V}$ is invariant under a large number of symmetries, and the examples given above show that $v \in \mathcal{V}$ itself may be symmetrical. For example, if $v(x, y) \in \mathcal{V}$,

then $v(y, x)$, $\overline{v(x, y)}$ (the complex conjugate of $v(x, y)$), $v(x, \omega y)$ and all combinations thereof are also in $\mathcal{V}$. Further, if $v = (f, g), v' = (f', g') \in \mathcal{V}$, then there is a natural composition, implicit already in the iterations of (1.2). To be specific, we define $w = (h, k) = v \circ v'$, by

$$(1.11) \qquad h(x, y) = f(f'(x, y), g'(x, y)), \quad k(x, y) = g(f'(x, y), g'(x, y))$$

It follows from

$$(1.12) \qquad \begin{aligned} h^3(x, y) + k^3(x, y) &= f^3(f'(x, y), g'(x, y)) + g^3(f'(x, y), g'(x, y)) \\ &= (f'(x, y))^3 + (g'(x, y))^3 = x^3 + y^3 \end{aligned}$$

that $v \circ v' \in \mathcal{V}$ as well. The connections among v_3, (1.10) and v_9 are equivalent to the equation $v_3 \circ v_3 = v_9$; it turns out that $v_3 \circ v_4 = v_4 \circ v_3 = v_{12}$. The homogeneous version of composition (which applies to infinite solutions as well) is given as follows. If $v = (p : q : r)$ and $v' = (p' : q' : r')$, then

$$(1.13) \quad v \circ v' = (p(p'(x, y), q'(x, y)) : q(p'(x, y), q'(x, y)) : r'(x, y)r(p'(x, y), q'(x, y))).$$

Thus, $d(v \circ v') = d(v)d(v')$, unless there are common factors in (1.13). It can be shown directly that this cannot happen, but it will also follow from our main work.

The first principal result of this paper is the following theorem.

Theorem 1.1. *Under the usual addition on elliptic curves (see Section 2 for more details), $\mathcal{V}$ is an abelian group isomorphic to $\mathbb{Z} + \mathbb{Z} + \mathbb{Z}/3\mathbb{Z}$. The generators of infinite order may be taken to be $h_1 = (x, y)$ and $h_2 = (\omega x, \omega y)$; the element of order 3 is $h_0 = (1 : -\omega : 0)$, a solution of (1.4) "at infinity". Further, $d(mh_1 + nh_2 + th_0) = m^2 - mn + n^2$.*

Moreover, the subgroup $\mathcal{V}_1 = \{mh_1 + nh_2\}$ is ring-isomorphic to $\mathbb{Z}[\omega]$ under the identification $R(mh_1 + nh_2) = m + n\omega$, with addition on curves and composition in $\mathcal{V}_1$ corresponding to addition and multiplication in $\mathbb{Z}[\omega]$.

This result has myriad consequences on the nature of the solutions $(f(x, y), g(x, y))$; these are collected as our other main theorem.

Theorem 1.2.
  (1) *If $v \in \mathcal{V}$, then $(g(x, y))^3 = (f(y, x))^3$.*
  (2) *If $v, v' \in \mathcal{V}$, then $v \circ v'$ and $v' \circ v$ are affiliates.*
  (3) *If $v \in \mathcal{V}$, then $f, g \in \mathbb{Q}[\omega](x, y)$.*
  (4) *If $d(v) = 3d'$, then some affiliate of v can be written as $\tilde{v} \circ v_3$, where $d(\tilde{v}) = d'$. Hence there exist forms P, Q, R so that*

$$p(x, y) = P(x^3, y^3), \quad q(x, y) = Q(x^3, y^3), \quad r(x, y) = xyR(x^3, y^3)$$

  (5) *If $d(v) = 3d' + 1$, then, up to a permutation of (p, q), there exist forms P, Q, R so that*

$$p(x, y) = xP(x^3, y^3), \quad q(x, y) = yQ(x^3, y^3), \quad r(x, y) = R(x^3, y^3)$$

(6) *In no case is $d(v) \equiv 2 \pmod{3}$ and no monomial appearing in any p, q, r has an exponent congruent to 2 mod 3.*

(7) *The real solutions are precisely those of the form $v = mh_1$ for $m \in \mathbb{Z}$ and have $d(v) = m^2$. The solutions of the form $v = (f, \bar{f})$ are precisely those of the form mv_3 and have $d(v) = 3m^2$.*

(8) *If $f(d)$ denotes the number of solutions with degree d (counting each collection of affiliates as one solution), then*

$$(1.14) \qquad f(d) = \sum_{e|d} \left(\frac{e}{3} \right),$$

where $\left(\frac{\cdot}{3} \right)$ denotes the usual Legendre symbol. Thus, the degree of any solution has the form $m^2 \prod_j p_j$ where the p_j are primes $\equiv 0, 1 \pmod{3}$.

Here is the organization of the paper. In Section 2, we review the addition law for points on elliptic curves. This endows $\mathcal{V}$ with the structure of an abelian group. We then analyze a subgroup $\mathcal{V}_0$ of $\mathcal{V}$ and prove that Theorem 1.2 is true for $\mathcal{V}_0$. We define a ring isomorphism between a particular subset $\mathcal{V}_1$ of $\mathcal{V}$ (under addition and composition c.f. (1.11)) and the ring $\mathbb{Z}[\omega]$. In Section 3, we prove that another subset of $\mathcal{V}$, $\mathcal{V}_\infty$, is isomorphic to the endomorphism ring of the elliptic curve (1.4) and use this to prove that $\mathcal{V}_0 = \mathcal{V}$ and $\mathcal{V}_1 = \mathcal{V}_\infty$. In Section 4, we discuss the implication of these results for a few related Diophantine equations.

We remark that many (but not all) of these results can also be derived in an entirely elementary way. We shall present this approach in [6].

We also happily acknowledge helpful conversations with Bruce Berndt and Ken Ono, and we wish to thank the anonymous referee for helpful comments that improved the exposition.

2. Point addition

A general reference for this section is [9]. The first part of the presentation has been heavily influenced by [8], where addition is discussed on the curve $X^3 + Y^3 = A$. It is implicit in [8] that $A \in \mathbb{C}$, although this is formally unnecessary.

Addition is defined on elliptic curves using a few basic rules. If three points P, Q, R lie on a line, then $P + Q + R = 0$. This operation can be shown to be associative and the set of points on the curve forms an abelian group; see, e.g. [9, p.62]. This is even true if we look at "curves" whose coordinates are rational functions.

We consider the curve

$$(2.1) \qquad C : X^3 + Y^3 = A,$$

where for the moment we will be vague about the underlying space for (X, Y) and the nature of $A \neq 0$. The additive inverse is given by

$$(2.2) \qquad (X, Y) + (Y, X) = 0,$$

where 0 is the additive identity, to be identified below as a point at infinity on the curve. To find the explicit value of the sum, we parameterize the line through two points on C. If $(X_1, Y_1), (X_2, Y_2) \in C$, $(X_1, Y_1) \neq (X_2, Y_2)$, then the condition $\lambda(X_1, Y_1) + (1 - \lambda)(X_2, Y_2) \in C$ implies that

$$(\lambda X_1 + (1 - \lambda)X_2)^3 + (\lambda Y_1 + (1 - \lambda)Y_2)^3 = A$$

$$= (\lambda^3 + (1 - \lambda)^3)A + 3\lambda(1 - \lambda)A \implies$$

$$(2.3) \qquad \lambda(1 - \lambda)\left(\lambda(X_1^2 X_2 + Y_1^2 Y_2) + (1 - \lambda)(X_1 X_2^2 + Y_1 Y_2^2) - A\right) = 0$$

$$\implies \lambda = 0, \lambda = 1 \text{ or } \lambda = \frac{A - (X_1 X_2^2 + Y_1 Y_2^2)}{(X_1^2 X_2 + Y_1^2 Y_2) - (X_1 X_2^2 + Y_1 Y_2^2)},$$

provided $X_1^2 X_2 + Y_1^2 Y_2 \neq X_1 X_2^2 + Y_1 Y_2^2$. Ignoring $\lambda = 0, 1$, and assuming this condition holds, we have

$$(2.4) \qquad\qquad (X_1, Y_1) + (X_2, Y_2) + (W, Z) = 0,$$

where

$$(2.5) \qquad \begin{aligned} W &= \frac{A(X_1 - X_2) + Y_1 Y_2(X_2 Y_1 - X_1 Y_2)}{(X_1^2 X_2 + Y_1^2 Y_2) - (X_1 X_2^2 + Y_1 Y_2^2)} \\ Z &= \frac{A(Y_1 - Y_2) + X_1 X_2(X_1 Y_2 - X_2 Y_1)}{(X_1^2 X_2 + Y_1^2 Y_2) - (X_1 X_2^2 + Y_1 Y_2^2)} \end{aligned}$$

and so

$$(2.6) \qquad\qquad (X_1, Y_1) + (X_2, Y_2) = (Z, W),$$

again provided that the denominator in (2.5) is not zero.

If $X_1^2 X_2 + Y_1^2 Y_2 = X_1 X_2^2 + Y_1 Y_2^2 = B$, say, then $(X_1 - X_2)^3 + (Y_1 - Y_2)^3 = A - 3B + 3B - A = 0$, hence $Y_1 - Y_2 = -\omega^j(X_1 - X_2)$ for $j = 0, 1$ or 2. If $X_1 = X_2$, then $Y_1 = Y_2$. Otherwise, $X_1 - X_2 \neq 0$ and

$$0 = X_1^2 X_2 + Y_1^2 Y_2 - (X_1 X_2^2 + Y_1 Y_2^2) = X_1 X_2(X_1 - X_2) + Y_1 Y_2(Y_1 - Y_2)$$

$$(2.7) \quad = (X_1 - X_2)(X_1 X_2 - \omega^j Y_1 Y_2) \implies X_1 X_2 - \omega^j Y_1(Y_1 + \omega^j(X_1 - X_2)) = 0$$

$$\implies -\omega^j(Y_1 + \omega^j X_1)(Y_1 - \omega^j X_2) = 0$$

If $Y_1 = -\omega^j X_1$, then $A = X_1^3 + Y_1^3 = 0$. Otherwise, $Y_1 = \omega^j X_2$ and so $Y_2 = \omega^j X_1$; thus, $(X_2, Y_2) = (\omega^{2j} Y_1, \omega^j X_1)$. To summarize: the three instances in which we cannot add distinct points according to (2.5) and (2.6) are

$$(2.8) \qquad (X_1, Y_1) + (Y_1, X_1), \quad (X_1, Y_1) + (\omega Y_1, \omega^2 X_1), \quad (X_1, Y_1) + (\omega^2 Y_1, \omega X_1).$$

Observe that, if $(X_2, Y_2) = (\omega^{2j} Y_1, \omega^j X_1)$, then the numerators of (W, Z) are, for $j = 0, 1, 2$,

$$(2.9) \qquad \begin{aligned} & A(Y_1 - \omega^j X_1) + \omega^{2j} X_1 Y_1(\omega^j X_1^2 - \omega^{2j} Y_1^2) \\ & A(X_1 - \omega^{2j} Y_1) - \omega^j X_1 Y_1(\omega^j X_1^2 - \omega^{2j} Y_1^2), \end{aligned}$$

respectively, and are in ratio $(1 : -w^{2j})$. In other words, (2.5) fails precisely when the sum would be one of the points at infinity. Accordingly, we add them to the definition of C and write

(2.10)
$$(X_1, Y_1) + (Y_1, X_1) + (1 : -1 : 0) = 0,$$
$$(X_1, Y_1) + (\omega Y_1, \omega^2 X_1) + (1 : -\omega^2 : 0) = 0,$$
$$(X_1, Y_1) + (\omega^2 Y_1, \omega X_1) + (1 : -\omega : 0) = 0.$$

Note that, for example, $(X_1 : Y_1 : 1), (Y_1 : X_1 : 1), (1 : -1 : 0)$ all lie on the projective line $(X_1 + Y_1)u_3 = u_1 + u_2$.

In view of (2.2), we see that $(1 : -1 : 0)$ is the additive identity and the point $h_0 := (1 : -\omega : 0)$ has order 3. Further, we see that

(2.11) $\qquad (\omega X_1, \omega^2 Y_1) = (X_1, Y_1) + h_0, \qquad (\omega^2 X_1, \omega Y_1) = (X_1, Y_1) + 2h_0.$

We still need to define addition when $(X_1, Y_1) = (X_2, Y_2)$. In this case, we construct the equivalent to the tangent line to the point at (X_1, Y_1) to make a double point and decree that the third intersection point will be $-2(X_1, Y_1)$. Formal implicit differentiation says that the "slope" to the curve $X^3 + Y^3 = A$ at (X_1, Y_1) equals $-X_1^2/Y_1^2$, so we seek $\lambda \neq 0$ so that

(2.12)
$$(X_1 + \lambda)^3 + \left(Y_1 - \lambda \frac{X_1^2}{Y_1^2}\right)^3 - A = 0.$$

Since $X_1^3 + Y_1^3 = A$, the left-hand side of (2.12) is divisible by λ^2, so

(2.13) $\qquad \lambda = \dfrac{3X_1 Y_1^3}{X_1^3 - Y_1^3} \implies -2(X_1, Y_1) = \left(\dfrac{X_1(A + Y_1^3)}{X_1^3 - Y_1^3}, \dfrac{-Y_1(A + X_1^3)}{X_1^3 - Y_1^3}\right).$

We now set $A = x^3 + y^3 \in \mathbb{C}[x, y]$ and summarize the foregoing discussion of addition. Addition involving points at infinity is specified by (2.2) and (2.11). Otherwise,

If $(X_1, Y_1) \neq (X_2, Y_2)$, then $(X_1, Y_1) + (X_2, Y_2) = (Z, W)$, where

(2.14)
$$Z = \frac{(x^3 + y^3)(Y_1 - Y_2) + X_1 X_2(X_1 Y_2 - X_2 Y_1)}{(X_1^2 X_2 + Y_1^2 Y_2) - (X_1 X_2^2 + Y_1 Y_2^2)},$$
$$W = \frac{(x^3 + y^3)(X_1 - X_2) + Y_1 Y_2(X_2 Y_1 - X_1 Y_2)}{(X_1^2 X_2 + Y_1^2 Y_2) - (X_1 X_2^2 + Y_1 Y_2^2)};$$
$$\text{Otherwise, } 2(X_1, Y_1) = \left(\frac{-Y_1(2X_1^3 + Y_1^3)}{X_1^3 - Y_1^3}, \frac{X_1(X_1^3 + 2Y_1^3)}{X_1^3 - Y_1^3}\right).$$

Note that $2(X_1, Y_1) = (X_1, Y_1) \circ (-v_4)$, and that in the extract cited in the Introduction, Viète in [10], in effect, chooses a slope for the line to ensure that the cubic equation for λ would have a double root at $\lambda = 0$, rendering its third root easy to find. (This tangent line was computed almost 100 years before calculus was invented!) Silverman [8, p.335] explicitly derived (2.13), with regards to elliptic curves of the form $x^3 + y^3 = A$ with $A \in \mathbb{C}$, although he did not make the reference to Viète.

Finally, since $\omega^2 = \lambda + (1 - \lambda)\omega$ for $\lambda = -\omega$, we observe that

$$(X_1, Y_1) + (X_1, \omega Y_1) + (X_1, \omega^2 Y_1) = 0$$

(2.15)
$$(X_1, Y_1) + (\omega X_1, Y_1) + (\omega^2 X_1, Y_1) = 0$$

$$(X_1, Y_1) + (\omega X_1, \omega Y_1) + (\omega^2 X_1, \omega^2 Y_1) = 0.$$

We now specialize this discussion to $\mathcal{V}$. First, we write the affiliates of $(f, g) \in \mathcal{V}$ in arrays to clarify these sums to zero over lines. Write $(f, g) = e_1$ and $(\omega f, \omega g) = e_2$ for short. Then all affiliates can be expressed in terms of e_1, e_2 and h_0:

$$(f, \omega^2 g) = e_2 + 2h_0 \qquad (\omega f, \omega^2 g) = e_1 + h_0 \qquad (\omega^2 f, \omega^2 g) = -e_1 - e_2$$

$$(f, \omega g) = -e_1 - e_2 + h_0 \quad (\omega f, \omega g) = e_2 \qquad (\omega^2 f, \omega g) = e_1 + 2h_0$$

$$(f, g) = e_1 \qquad\qquad (\omega f, g) = -e_1 - e_2 + 2h_0 \quad (\omega^2 f, g) = e_2 + h_0$$

(2.16)

$$(g, \omega^2 f) = -e_2 + 2h_0 \qquad (\omega g, \omega^2 f) = -e_1 + h_0 \qquad (\omega^2 g, \omega^2 f) = e_1 + e_2$$

$$(g, \omega f) = e_1 + e_2 + h_0 \qquad (\omega g, \omega f) = -e_2 \qquad (\omega^2 g, \omega f) = -e_1 + 2h_0$$

$$(g, f) = -e_1 \qquad\qquad (\omega g, f) = e_1 + e_2 + 2h_0 \qquad (\omega^2 g, f) = -e_2 + h_0.$$

We now recall h_0 and identify two special points on $\mathcal{V}$:

(2.17) $\qquad\qquad h_0 = (1 : -\omega : 0), \qquad h_1 = (x, y), \qquad h_2 = (\omega x, \omega y),$

and let

(2.18) $\qquad\qquad \mathcal{V}_0 = \{mh_1 + nh_2 + th_0 \ : \ m, n \in \mathbb{Z}, \ t \in \{0, 1, 2\}\},$

where $mh_1 + nh_2 + th_0$ is the *canonical* expression for $(f, g) \in \mathcal{V}_0$. (We henceforth reserve m, n, t to the description above.) We also recall the definition of an important subset of $\mathcal{V}_0$:

(2.19) $\qquad\qquad \mathcal{V}_1 = \{mh_1 + nh_2 \ : \ m, n \in \mathbb{Z}\}.$

For $(0, 0) \neq (m, n) \in \mathbb{Z}^2$, let

(2.20) $\qquad T(m, n) = \{mh_1 + nh_2, mh_1 + nh_2 + h_0, mh_1 + nh_2 + 2h_0\}$

denote the (m, n)-*trio*.

We now begin to describe the ring-isomorphism between $\mathcal{V}_1$ and $\mathbb{Z}[\omega]$ by analyzing $v \circ w$. Our first results apply to V_0 as well.

Lemma 2.1. *If $v = (f, g) \in \mathcal{V}$, then*

(2.21) $h_1 \circ v = v \circ h_1 = v, \quad h_2 \circ v = v \circ h_2 = \omega v, \quad h_2 \circ h_2 = \omega h_2 = \omega^2 h_1 = -h_1 - h_2.$

Proof. The first identity is immediate from the definition of composition. For the second one, note that f and g are homogeneous of degree 1, hence $f(\omega x, \omega y) = \omega f(x, y)$ and $g(\omega x, \omega y) = \omega g(x, y)$, so

(2.22) $\qquad v \circ h_2 = (f(\omega x, \omega y), g(\omega x, \omega y)) = (\omega f(x, y), \omega g(x, y)) = h_2 \circ v.$

The final equation follows from the second and (2.15). $\qquad\qquad\square$

We now make a simple, but consequential observation about left-distributivity.

Lemma 2.2. *If $v, v', w \in \mathcal{V}$ and $\tilde{v} = v + v'$, then $\tilde{v} \circ w = v \circ w + v' \circ w$. Thus, $(mv + nv') \circ w = mv \circ w + nv' \circ w$.*

Proof. Suppose $w = (f(x, y), g(x, y))$. Composition with w amounts to the formal substitution $(x, y) \to (f(x, y), g(x, y))$; (1.11) shows that substitution this is preserved by the varying definitions of addition, establishing the first assertion. The second assertion follows from the first by induction. □

Theorem 2.3. *If $v = (f, g) = mh_1 + nh_2 + th_0 \in \mathcal{V}_0$, then*

$$(2.23) \quad (\omega f, \omega g) = -nh_1 + (m - n)h_2 + th_0, \quad (\omega^2 f, \omega^2 g) = (n - m)h_1 - mh_2 + th_0.$$

Proof. Lemmas 2.1 and 2.2 imply that

$$(2.24) \quad (\omega f, \omega g) = \omega v = v \circ h_2 = mh_1 \circ h_2 + nh_2 \circ h_2 + th_0 \circ h_2 = mh_2 + n(-h_1 - h_2) + th_0.$$

The other equation follows from (2.15). □

For $x = mh_1 + nh_2 \in \mathcal{V}_1$, define

$$(2.25) \quad R(x) = R(mh_1 + nh_2) = m + n\omega$$

Note that if $v = mh_1 + nh_2 \in \mathcal{V}_1$, then Theorem 2.3 implies that

$$(2.26) \quad R(\omega v) = -n + (m - n)\omega = \omega(m + n\omega) = \omega R(v).$$

Using (2.16) and Theorem 2.3, once we know the canonical expression for (f, g), we know the canonical expressions for all of its affiliates. The canonical expressions for the solutions listed in the introduction are

$$(2.27) \quad \begin{array}{c} v_1 = h_1, \quad v_3 = h_1 + 2h_2, \quad v_4 = -2h_1, \\ v_7 = -2h_1 - 3h_2, \quad v_9 = -3h_1, \quad v_{12} = -2h_1 - 4h_2. \end{array}$$

Note that $R(v_1) = 1$, $R(v_3) = 1 + 2\omega = \omega - \omega^2 = i\sqrt{3}$ and $R(v_4) = -2$.

It is clear from (2.16) and Theorem 2.3 that each set of 18 affiliates is a union of the six trios:

$$(2.28) \quad \begin{array}{c} T(m, n), \quad T(-m, -n), \quad T(-n, m - n), \\ T(n, n - m), \quad T(n - m, -m), \quad T(m - n, m), \end{array}$$

and every $v \in \mathcal{V}_0$ is in a trio with some $w \in \mathcal{V}_1$. As long as $(m, n) \neq (0, 0)$, the six trios in (2.28) are distinct.

The argument of Theorem 2.3 extends to give a closed form for composition in $\mathcal{V}$.

Theorem 2.4. *If $v = mh_1 + nh_2 + th_0$ and $v' = m'h_1 + n'h_2 + t'h_0$, then*

$$(2.29) \quad \begin{aligned} v \circ v' &= m(m'h_1 + n'h_2 + t'h_0) + n(-n'h_1 + (m' - n')h_2 + t'h_0) + th_0 \\ &= (mm' - nn')h_1 + (mn' + m'n - nn')h_2 + ((m + n)t' + t)h_0. \end{aligned}$$

Proof. Since $v \circ v' = mh_1 \circ v' + nh_2 + th_0 \circ v'$, three applications of Lemma 2.2, keeping (2.21) in mind, give the result. □

We note a crucial implication of Theorem 2.4 for elements of $\mathcal{V}_1$ ($t = t' = 0$):

$$(2.30) \qquad R(v \circ v') = (mm' - nn') + \omega(mn' + m'n - nn') = R(v)R(w).$$

For $y \in \mathbb{Z}[\omega]$, let $N(y)$ denote the usual norm. We have

$$(2.31) \quad \Phi(m, n) := N(m + n\omega) = |m + n\omega|^2 = (m + n\omega)(m + n\omega^2) = m^2 - mn + n^2.$$

Since $N(y) = N(\pm\omega^j y)$, we have

$$(2.32) \qquad \begin{aligned} \Phi(m, n) &= \Phi(-m, -n) = \Phi(-n, m - n) = \Phi(n, n - m) \\ &= \Phi(n - m, m) = \Phi(m - n, -m). \end{aligned}$$

Further, (2.30) implies that

$$(2.33) \qquad \Phi(mm' - nn', mn' + m'n - nn') = \Phi(m, n)\Phi(m', n');$$

of course, (2.32) and (2.33) can also be verified directly. It will follow from Theorem 1.1 that $\mathcal{V}_0 = \mathcal{V}$ and

$$(2.34) \qquad d(mh_1 + nh_2 + th_0) = \Phi(m, n) := m^2 - mn + n^2.$$

Corollary 2.5. *If $v, v' \in \mathcal{V}$ are given as above, then*

$$(2.35) \qquad v \circ v' - v' \circ v = (((m + n)t' + t) - ((m' + n')t + t'))h_0$$

so $v \circ v'$ and $v' \circ v$ are in the same trio. Furthermore, $v \circ v' = v' \circ v$ if and only if $(m + n - 1)t' \equiv (m' + n' - 1)t \pmod{3}$, in particular, if $v, v' \in \mathcal{V}_1$.

We also remark that Theorem 2.4 and the to-be-proved formula (2.34) combine to imply that $d(v \circ v') = d(v)d(v')$, so that no cancellation occurs in the composition. We note one more corollary to 2.4, which follows from the bi-homogeneity in the pairs of variables (m, n) and (m', n') of (2.29) for elements of $\mathcal{V}_1$; the corollary is not generally true in $\mathcal{V}$.

Corollary 2.6. *For $v, v' \in \mathcal{V}_1$ and $r \in \mathbb{Z}$, $(rv) \circ v' = v \circ (rv') = r(v \circ v')$. In particular, taking $v' = h_1$, we have $rv = v \circ (rh_1)$.*

Theorem 2.7. *The map R is a ring isomorphism between $\mathcal{V}_1$ (with the operations of point-addition and composition) and $\mathbb{Z}[\omega]$. Furthermore, with the appropriate definitions of multiplication by ω and the usual complex conjugation,*

$$(2.36) \qquad R(\omega v) = \omega R(v), \qquad R(\overline{v}) = \overline{R(v)}.$$

Proof. That $\mathcal{V}_1$ is a ring with respect to addition and composition follows from Lemma 2.2 in one direction (and from Corollary 2.5 in the other). We remark that Corollary 2.5 implies that the full set $\mathcal{V}$ itself is not a ring with composition as "multiplication", because the right-distributive law fails. In particular, if $v, v' \in \mathcal{V}$ then by (1.13), $h_0 = h_0 \circ v = h_0 \circ v' = h_0 \circ (v + v')$, but $h_0 \neq 2h_0$.

Clearly, R is a bijection and $R(v + w) = R(v) + R(w)$. If $v = mh_1 + nh_2$ and $w = m'h_1 + n'h_2$, then as we have seen in (2.30), $R(v \circ w) = R(v)R(w)$. That $R(\omega v) = \omega R(v)$ was shown in equation (2.26). For the second statement, we needn't

concern ourselves with points at infinity, and the exact formulas of (2.14) imply that complex conjugation factors through addition, so that

(2.37) $\qquad (X_1, Y_1) + (X_2, Y_2) = (Z, W) \implies \overline{(X_1, Y_1)} + \overline{(X_2, Y_2)} = \overline{(Z, W)}.$

Since $\overline{h_1} = h_1$ and $\overline{h_2} = \overline{(\omega x, \omega y)} = (\omega^2 x, \omega^2 y) = \omega h_2 = -h_1 - h_2$, we see that if $v = mh_1 + nh_2$, then

(2.38)
$$\overline{v} = mh_1 + n(-h_1 - h_2) \implies$$
$$R(\overline{v}) = m + n(-1 - \omega) = m + n\omega^2 = \overline{m + n\omega} = \overline{R(v)}.$$

$\qquad\square$

Corollary 2.8. *If $v = m_0 h_1 + n_0 h_2 \in \mathcal{V}_1$ and $w = m_1 h_1 + n_1 h_2$, then there exists $v' \in \mathcal{V}$ such that $v = v' \circ w$ if and only if $\frac{m_0 + n_0\omega}{m_1 + n_1\omega} \in \mathbb{Z}[\omega]$; that is, if and only if*

(2.39) $\qquad m_0 m_1 + n_0 n_1 \equiv m_0 n_1 \equiv m_1 n_0 \pmod{m_1^2 - m_1 n_1 + n_1^2}$

Proof. A routine calculation shows that

(2.40) $\qquad \dfrac{m_0 + n_0\omega}{m_1 + n_1\omega} = \dfrac{m_0 m_1 + n_0 n_1 - m_0 n_1 + (m_1 n_0 - m_0 n_1)\omega}{m_1^2 - m_1 n_1 + n_1^2}.$

$\qquad\square$

Corollary 2.9. *If $v = mh_1 + nh_2 \in \mathcal{V}_1$, then*

(2.41) $\qquad v \circ \overline{v} = N(R(v)) h_1 = (m^2 - mn + n^2) h_1.$

Proof. It follows from (2.38) that $R(v)R(\overline{v}) = N(R(v))$. $\qquad\square$

If particular, since $g_3 = \overline{f_3}$, $\overline{v}_3 = -v_3$ and we recover that $v_3 \circ v_3 = v_9$. It follows from (2.38) that $\overline{mh_1} = mh_1$ for all $m \in \mathbb{Z}$; thus Corollary 2.9 implies that each $v \in \mathcal{V}_1$ has a "composition multiple" which is real. Observe that $mh_1 + nh_2$ and $nh_1 + mh_2$ are not, in general, affiliates, although $\Phi(m, n) = \Phi(n, m)$.

Corollary 2.10. *If $v = mh_1 + nh_2$, then $\omega\overline{v} = nh_1 + mh_2$.*

Proof. This follows immediately from $n + m\omega = \omega(\overline{m + n\omega})$. $\qquad\square$

Corollary 2.11. *If $v \in \mathcal{V}_1$, then v and $\overline{v}$ are affiliates if and only if v is an affiliate of mv_1 or mv_3 for some integer m.*

Proof. This follows from a somewhat tedious comparison of (2.28) for (m, n) and (n, m). Equality holds if $mn(m - n) = 0$ or $(m + n)(m - 2n)(2m - n) = 0$, which give multiples of v_1 and v_3 respectively. $\qquad\square$

We note that $\overline{mv_1} = mv_1$ and $\overline{mv_3} = -mv_3$. It follows that the number of solutions of degree d, $f(d)$, is even unless $d = m^2$ or $d = 3m^2$.

We now turn to proving Theorem 1.2 for points in $\mathcal{V}_0$, assuming Theorem 1.1. We show that assertions (1) through (6) hold for $v, w \in \mathcal{V}_1$; since the components of $v + th_0$ differ from v by powers of ω, which do not affect the assertions, the claimed results will also hold for $\mathcal{V}_0$.

Proof of Theorem 1.2. We start with (1). Let $v = mh_1 + nh_2$ and $v' = (y, x) = -h_1$. Then $v \circ v' = (f(y, x), g(y, x))$ by (1.11). On the other hand, $R(v \circ v') = R(v)R(v') = -R(v) = -m - n\omega = R(-v)$, hence $v \circ v' = -v$; that is, $(f(y, x), g(y, x)) = (g(x, y), f(x, y))$.

Item (2) is Corollary 2.5.

Item (3) follows from Theorem 1.1 together with the observation (from (2.14)) that if v and v' have coefficients in $\mathbb{Q}(\omega)$, then so does $v + v'$.

To prove (4), let $v = mh_1 + nh_2$ and note that $d(v) = (m + n)^2 - 3mn \equiv 0 \pmod{3}$ implies that $m + n \equiv 0 \pmod{3}$. Applying (2.39) from Corollary 2.8 gives $-m - 2n \equiv -2m \equiv -n \pmod{3}$ as a condition for the existence of $v' \in \mathcal{V}_1$ so that $v = v' \circ v_3$, and these are satisfied when $3 \mid m + n$. If $v' = (\frac{p'}{r'}, \frac{q'}{r'})$, then by (1.13),

$$
\begin{aligned}
p(x, y) &= p'(\zeta^{-1} x^3 + \zeta y^3, \zeta x^3 + \zeta^{-1} y^3), \\
q(x, y) &= q'(\zeta^{-1} x^3 + \zeta y^3, \zeta x^3 + \zeta^{-1} y^3), \\
r(x, y) &= \sqrt{3}\, xy\, r'(\zeta^{-1} x^3 + \zeta y^3, \zeta x^3 + \zeta^{-1} y^3),
\end{aligned}
$$
(2.42)

which verifies the asserted shape. (Compare with the earlier discussion of (1.10).)

Next, we prove (5). Since $(m + n)^2 \equiv d(v) \equiv 1 \pmod{3}$, for one choice of sign (say $+$), we have $\pm v = mh_1 + nh_2$, where $m + n \equiv 1 \pmod{3}$. (The choice of sign amounts to a possible permutation of f and g.) Let $v = (f, g) = (p/r, q/r)$. Since $(\omega x, y) = -h_1 - h_2 + 2h_0$, Theorem 2.4 now implies that

$$
v \circ (\omega x, y) = (n - m)h_1 - mh_2 + 2(m + n)h_0 = (n - m)h_1 - mh_2 + 2h_0,
$$

which by (2.16) and Theorem 2.3 equals $(\omega f, g)$. In other words,

$$
\left(\frac{p(\omega x, y)}{r(\omega x, y)}, \frac{q(\omega x, y)}{r(\omega x, y)} \right) = \left(\omega \frac{p(x, y)}{r(x, y)}, \frac{q(x, y)}{r(x, y)} \right).
$$
(2.43)

Thus, $p(\omega x, y)r(x, y) = \omega p(x, y)r(\omega x, y)$ and $q(\omega x, y)r(x, y) = q(x, y)r(\omega x, y)$. Since $p(x, y)$ and $r(x, y)$ are relatively prime, we have $p(x, y) \mid p(\omega x, y)$; since they have the same degree, it follows that $p(\omega x, y) = c_p p(x, y)$ for $c_p \in \mathbb{C}$. Similarly, $q(\omega x, y) = c_q q(x, y)$ and $r(\omega x, y) = c_r r(x, y)$. Since $p, q, r \neq 0$, examination at any non-zero monomial shows that each constant is a power of ω and so all powers of x occurring in p with non-zero coefficient are congruent modulo 3, and similarly for q and r. Since $d \equiv 1 \pmod{3}$, the choices are $p(x, y) = xP(x^3, y^3), yP(x^3, y^3)$ or $x^2 y^2 P(x^3, y^3)$ for some polynomial P; $q(x, y) = xQ(x^3, y^3), yQ(x^3, y^3)$ or $x^2 y^2 Q(x^3, y^3)$ for some polynomial Q; and $r(x, y) = R(x^3, y^3), xy^2 R(x^3, y^3)$ or $x^2 y R(x^3, y^3)$ for some polynomial R. Since p and q are relatively prime, there cannot be a common factor of x or y, hence $(p(x, y), q(x, y))$ is either $(xP(x^3, y^3), yQ(x^3, y^3))$ or $(yP(x^3, y^3), xQ(x^3, y^3))$. Upon dividing the components of either side of (2.43), we find that

$$
\frac{p(\omega x, y)}{q(\omega x, y)} = \omega \frac{p(x, y)}{q(x, y)},
$$
(2.44)

hence $p(x, y) = xP(x^3, y^3)$ and $q(x, y) = yQ(x^3, y^3)$; (2.43) now implies that $r(x, y) = r(\omega x, y)$, so $r(x, y) = R(x^3, y^3)$.

Item (6) follows immediately from (4) and (5).

To prove (7), note that (2.11) $\overline{h_0} = \overline{(1 : -\omega : 0)} = (1 : -\omega^2 : 0) = 2h_0$ and so (2.11) and Theorem 2.7 imply that

$$(2.45) \qquad \overline{mh_1 + nh_2 + th_0} = mh_1 + n(-h_1 - h_2) + t(2h_0).$$

If v is real, then $v = \overline{v}$ so that $nh_1 + 2nh_2 - th_0 = 0$, hence $n = t = 0$. Note also that if $v = (f, g) = rh_1$, then $f, g \in \mathbb{Q}(x, y)$.

Finally, we turn to (8). Since each solution has 18 affiliates and Theorem 1.1 implies that $d(mh_1 + nh_2 + th_0) = m^2 - mn + n^2$, $t \in \{0, 1, 2\}$, we have

$$(2.46) \qquad 1 + 6\sum_{d=1}^{\infty} f(d)z^d = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} z^{m^2-mn+n^2}.$$

It is fairly well-known that

$$(2.47) \qquad \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} z^{m^2-mn+n^2} = 1 + 6\sum_{i=0}^{\infty} \left(\frac{z^{3i+1}}{1 - z^{3i+1}} - \frac{z^{3i+2}}{1 - z^{3i+2}} \right).$$

The equations (2.46) and (2.47) combine to imply (1.14). The identity (2.47) has a convoluted history, as described by our colleague Bruce Berndt in, for example, [1, p.78] and [2, pp.196-199], and by Hirschhorn in [4]. Its arithmetical equivalent is a special case of an 1840 theorem of Dirichlet. It was found independently by Lorenz and Ramanujan.

It follows from (1.14) that $f(p^k) = k + 1$ if $p \equiv 1 \pmod 3$; if $p \equiv 2 \pmod 3$, then $f(p^k)$ equals 0 or 1, depending on whether k is odd or even. Since $f(d)$ is multiplicative, $f(n) > 0$ implies that no prime $\equiv 2 \pmod 3$ can appear to an odd power in the prime factorization of n. We note also that $\{f(n)\}$ is unbounded as $n \to \infty$. Since the taxicab number $1729 = 7 \cdot 13 \cdot 19$, we have $f(1729) = 8$: there are 8 solutions to (1.4) in which p and q have degree 1729. □

3. Proof of Theorem 1.1

In this section, we will prove Theorem 1.1. We will consider solutions to

$$E : p^3 + q^3 = (x^3 + y^3)r^3$$

where $0 \neq p, q, r \in \mathbb{C}[x, y]$ are homogeneous polynomials with $\deg(p) = \deg(q) = \deg(r) - 1$.

For such a point $P = (a(x, y) : b(x, y) : c(x, y))$, the map

$$\phi_P(p : q : r) = (a(p, q) : b(p, q) : c(p, q)r)$$

is a morphism from E to itself. There are two basic properties that immediately follow from the definition. First,

$$(3.1) \qquad \phi_P(x : y : 1) = (a(x, y) : b(x, y) : c(x, y)) = P.$$

Second, for any point P, the map ϕ_P permutes the points at infinity: $(1 : -1 : 0)$, $(1 : -\omega : 0)$ and $(1 : -\omega^2 : 0)$.

Before we continue, we need a lemma.

Lemma 3.1. *The point $P = (x : y : 1) \in \mathcal{V}$ has infinite order.*

Proof. Define the homomorphism $\phi : E \to E'$ by setting $x = 2$ and $y = 1$. Thus

$$E' : p^3 + q^3 = 9r^3.$$

We have $\phi((x : y : 1)) = (2 : 1 : 1)$. Using standard techniques (e.g. Prop. VII.3.1(b) or Cor. VIII.7.2 in [9]), one can compute that $E'(\mathbb{Q})$, the group of rational points on E', is isomorphic to $\mathbb{Z}$, and is generated by $(2 : 1 : 1)$. It follows that P has infinite order, since a homomorphic image of P also has infinite order. $\square$

Let $\mathcal{V}_\infty = \{P \in \mathcal{V} : \phi_P(0) = 0\}$ be the subgroup of points $P \in \mathcal{V}$ so that ϕ_P fixes the chosen point at infinity. Recall that any polynomial map $\phi : E \to E$ with $\phi(0) = 0$ is called an *isogeny*. Theorem III.4.8 of [9] implies that if ϕ is an isogeny, then $\phi(P + Q) = \phi(P) + \phi(Q)$. The set of all isogenies from E to itself is denoted $\text{End}(E)$ and is called the endomorphism ring of E. The two ring operations are addition (in the group law, so $(\phi_1 + \phi_2)(R) = \phi_1(R) + \phi_2(R)$), and function composition. Our approach to proving Theorem 1.1 will be to define a ring structure on $\mathcal{V}_\infty$, and prove that $\mathcal{V}_\infty \cong \text{End}(E)$, and finally show that $\mathcal{V}_\infty = \mathcal{V}_1 = \{mh_1 + nh_2 : m, n \in \mathbb{Z}\}$.

Lemma 3.2. *For any two points $P, Q \in \mathcal{V}$, we have*

$$\phi_{P+Q} = \phi_P + \phi_Q.$$

Proof. From (3.1), we have

$$\begin{aligned}
\phi_{P+Q}(x : y : 1) &= P + Q \\
&= \phi_P(x : y : 1) + \phi_Q(x : y : 1).
\end{aligned}$$

Thus, the point $(x : y : 1)$ is sent to 0 under the map $\phi_{P+Q} - \phi_P - \phi_Q$. If $S = \phi_{P+Q}(0) - \phi_P(0) - \phi_Q(0)$, then $F = \phi_{P+Q} - \phi_P - \phi_Q - S$ is a morphism from E to itself that fixes 0. Thus, F is an isogeny. Any morphism between two curves is either constant, or each point has finitely many preimages. It follows that $\ker F$ is either finite, or all of E. Since F is an isogeny,

$$F([3n](x : y : 1)) = [3n]F((x : y : 1)) = [3n](-S) = [n]([3](-S)) = 0.$$

Here, and in the rest of the section, $[m](p : q : r)$ is used instead of $m(p : q : r)$ for clarity. By Lemma 3.1, $(x : y : 1)$ has infinite order, and hence the kernel of F is infinite. This implies that F is the zero map, and so

$$\phi_{P+Q}(R) - \phi_P(R) - \phi_Q(R) = S.$$

for any R. Setting $R = (x : y : 1)$ we see that $S = 0$, and $\phi_{P+Q} = \phi_P + \phi_Q$. $\square$

Recall that $h_0 = (1 : -\omega : 0) \in \mathcal{V}$ and $2h_0 = (1 : -\omega^2 : 0)$. Clearly

$$\phi_{h_0}(R) = h_0, \qquad \phi_{2h_0}(R) = 2h_0$$

for all $R \in \mathcal{V}$. It follows that for any point $P \in \mathcal{V}$, either P, $P - h_0$ or $P - 2h_0 \in \mathcal{V}_\infty$. Hence,

$$\mathcal{V} \cong \mathcal{V}_\infty \times \langle h_0 \rangle.$$

Lemma 3.3. *The subgroup $\mathcal{V}_\infty \subseteq \mathcal{V}$ can be given the structure of a ring by defining $P \cdot Q = \phi_P(Q)$.*

Proof. We know that $\mathcal{V}_\infty$ is an abelian group. We must show that the multiplication operator is associative and distributive. By (3.1),

$$\phi_P(x : y : 1) = P,$$

we have

$$P \cdot Q = \phi_P(Q) = \phi_P(\phi_Q(x : y : 1)).$$

Since $\phi_S(x : y : 1) = S$ for any $S \in \mathcal{V}$, it follows that $\phi_{P \cdot Q}(x : y : 1) = P \cdot Q = \phi_P(\phi_Q(x : y : 1))$. Thus, $(x : y : 1)$ is in the kernel of the isogeny $\phi_{P \cdot Q} - \phi_P \circ \phi_Q$. By Lemma 3.1, the kernel is therefore infinite and hence $\phi_{P \cdot Q} = \phi_P \circ \phi_Q$. The associativity then follows from the fact that function composition is associative. To prove the distributive law, we use that ϕ_P is an isogeny and hence

$$\begin{aligned}
P \cdot (Q + R) &= \phi_P(Q + R) \\
&= \phi_P(Q) + \phi_P(R) \\
&= (P \cdot Q) + (P \cdot R).
\end{aligned}$$

Thus, $\mathcal{V}_\infty$ naturally has the structure of a ring. $\square$

Lemma 3.4. *The map $\tau : \mathcal{V}_\infty \to \operatorname{End}(E)$ given by*

$$\tau(P) = \phi_P$$

is an isomorphism of rings.

Proof. Lemma 3.2 implies that $\tau(P + Q) = \tau(P) + \tau(Q)$. In the proof of Lemma 3.3, we showed that $\tau(P \cdot Q) = \tau(P) \circ \tau(Q)$. Thus, τ is a ring homomorphism. If $\tau(P) = 0$, then $\phi_P = 0$ and so $\phi_P((x : y : 1)) = P = 0$. Hence, τ is injective.

Conversely, if $\phi \in \operatorname{End}(E)$, and $P = \phi(x : y : 1)$, then $\phi - \phi_P$ has $(x : y : 1)$ in its kernel. Thus, the kernel of $\phi - \phi_P$ is infinite and hence $\phi = \phi_P$. It follows that $\phi = \tau(P)$ and so τ is surjective. $\square$

A similar argument identifying the Mordell-Weil group of an elliptic surface with the endomorphism ring was given by Frank de Zeeuw in his master's thesis [11].

Now, we will prove our main result.

Proof of Theorem 1.1. In light of the fact that

$$\mathcal{V} \cong \mathcal{V}_\infty \times \langle T \rangle,$$

and that $\mathcal{V}_\infty$ is isomorphic to $\text{End}(E)$ by Lemma 3.4, it suffices to determine $\text{End}(E)$. Theorem VI.6.1(b) of [9] states that if E is an elliptic curve defined over a field of characteristic zero, then $\text{End}(E)$ is isomorphic to either $\mathbb{Z}$ or an order in an imaginary quadratic field. Observe that $\text{End}(E)$ contains the map defined by

$$\phi((p : q : r)) = (\omega p : \omega q : r).$$

Hereafter we will refer to the map ϕ as $[\omega]$. This map fixes $(1 : -1 : 0)$, satisfies $[\omega]^3 = 1$, and sends $(x : y : 1)$ to $(\omega x : \omega y : 1)$. It follows that $\text{End}(E) \cong \mathbb{Z}[\omega]$ and

$$\mathcal{V}_\infty = \mathcal{V}_1 = \langle (x : y : 1), (\omega x : \omega y : 1) \rangle \cong \mathbb{Z} \times \mathbb{Z}.$$

Now, we will prove that $d(mh_1 + nh_2 + th_0) = m^2 - mn + n^2$. It suffices to prove this with $t = 0$, since $mh_1 + nh_2$ is an affiliate of $mh_1 + nh_2 + th_0$.

If $P := mh_1 + nh_2 \in \mathcal{V}_\infty$, it is easy to see that the degree of P is the same as the degree of the map $\phi_P : E \to E$. In this case,

$$\begin{aligned}
\phi_P((x : y : 1)) &= mh_1 + nh_2 \\
&= m(x : y : 1) + n(\omega x : \omega y : 1) \\
&= [m + n\omega](x : y : 1).
\end{aligned}$$

Thus, $\phi_P = [m + n\omega]$. The ring $\text{End}(E)$ is endowed with an involution $\hat{\ }$ that satisfies

$$\widehat{\lambda + \phi} = \hat{\lambda} + \hat{\phi}$$
$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$$
$$\phi \circ \hat{\phi} = [\deg \phi]$$

(see Theorem III.6.2 of [9]). This, together with the fact that $\deg([m]) = m^2$ implies that

$$[\hat{\omega}] = [\omega^2].$$

This implies that

$$[\widehat{m + n\omega}] = [m + n\omega^2]$$

and so

$$\begin{aligned}
[\deg([m + n\omega])] &= [m + n\omega][m + n\omega^2] \\
&= [m^2 + (mn\omega + mn\omega^2) + n^2] \\
&= [m^2 - mn + n^2].
\end{aligned}$$

Since the degree of P equals $\deg \phi_P = \deg[m + n\omega]$, we have that the degree of P is $m^2 - mn + n^2$, as desired. $\qquad\square$

4. Related results and open questions

We conclude with a brief discussion of some related Diophantine equations. It is classically known that if $F(x, y)$ is a binary cubic form, then after an invertible linear transformation in (x, y), $F(x, y)$ has one of the following three shapes: $x^3, x^3 + y^3, x^2 y$. It is natural to wonder whether there are solutions to (1.4) in the other two cases.

Theorem 4.1. *The equations*

$$(4.1) \qquad p^3(x, y) + q^3(x, y) = x^3 r^3(x, y),$$

$$(4.2) \qquad p^3(x, y) + q^3(x, y) = x^2 y\ r^3(x, y),$$

have no non-trivial solutions in forms $p, q, r \in \mathbb{C}[x, y]$.

Proof. Any solution to (4.1) would be a solution to the Fermat equation $X^n + Y^n = Z^n$ for $n = 3$ over $\mathbb{C}[t]$, upon setting $(x, y) = (1, t)$. The non-existence of such non-constant solutions was proved by Liouville in 1879. (See the exposition in [7, pp.263-265].)

Assume (4.2) has a solution and rewrite as

$$(4.3) \qquad x^2 y\ r^3 = (p + q)(p + \omega q)(p + \omega^2 q).$$

Let $\mathcal{F} = \{p + \omega^j q : j = 0, 1, 2\}$. Note that $\mathcal{F}$ is linearly dependent: $\sum \omega^j (p + \omega^j q) = 0$, hence any polynomial that divides two elements of $\mathcal{F}$ divides the third, and also divides p and q. Let (p_0, q_0, r_0) be a solution of (4.3) in which $d = \deg r_0$ is minimal. If $d = 0$, then p_0 and q_0 must be linear and the product of the elements in $\mathcal{F}$ is $x^2 y$, hence x must divide two of them, and so $x | p_0, q_0$, a contradiction. Now suppose $d \geq 1$ and suppose π is an irreducible factor of r_0. If π divides two elements of $\mathcal{F}$, then, as before, π divides p, q and $(p_0 : \pi, q_0/\pi : r_0/\pi)$ is a solution to (4.2) of lower degree. It follows that if π^m is a factor of r_0, then π^{3m} is concentrated in one member of $\mathcal{F}$. We may thus write $r_0 = s_0 s_1 s_2$ so that $s_j^3 | p_0 + \omega^j q_0$. Since the degrees of $\{p_0 + \omega^j q_0\}$ are equal, (4.3) implies that the three remaining factors, $\{x, x, y\}$, are either dispersed, one to each $p_0 + \omega^j q_0$, or combined in a single factor. In the first case, we may again conclude that $x | p_0, q_0$, and (4.3) implies that $x | r_0$, a contradiction. In the second case, suppose without loss of generality that $x^2 y | p_0 + q_0$. Then we have $p_0 + q_0 = x^2 y\ s_0^3$, $p_0 + \omega q_0 = s_1^3$, $p_0 + \omega^2 q_0 = s_2^3$, and the linear dependence on the elements of $\mathcal{F}$ implies that

$$(4.4) \qquad x^2 y s_0^3 = -\omega s_1^3 - \omega^2 s_2^3,$$

which, after the absorption of constants, is a solution to (4.2). If $\deg s_1 = d$, then $\deg s_2 = d$, $\deg s_0 = d - 1$ and $\deg r = \deg s_0 + \deg s_1 + \deg s_2 = 3d - 1 > d$, contradicting its supposed minimality and completing the descent. $\qquad \square$

We now show that Theorem 1.2(4,5) contains, in effect, the solution to two other Diophantine equations.

Theorem 4.2. *Any solution in forms $a, b, c \in \mathbb{C}[x, y]$ to either of the equations*

$$(4.5) \qquad\qquad a^3(x, y) + b^3(x, y) = xy(x + y)\, c^3(x, y),$$

$$(4.6) \qquad\qquad x\, a^3(x, y) + y\, b^3(x, y) = (x + y)\, c^3(x, y)$$

can be directly derived from a solution to (1.4).

Proof. If (4.5) holds, then by taking $(x, y) \mapsto (x^3, y^3)$, we see that

$$(4.7) \qquad\qquad a^3(x^3, y^3) + b^3(x^3, y^3) = x^3 y^3 (x^3 + y^3) c^3(x^3, y^3),$$

hence $(a(x^3, y^3) : b(x^3, y^3) : xy\, c(x^3, y^3)) \in \mathcal{V}$, and $\deg(a(x^3, y^3)) = 3d'$. In the language of Theorem 1.2(4), we have $(a, b, c) = (P, Q, R)$; again, compare with (1.10).

Similarly, suppose (4.6) holds; take $(x, y) \mapsto (x^3, y^3)$ to obtain

$$(4.8) \qquad\qquad x^3\, a^3(x^3, y^3) + y^3\, b^3(x^3, y^3) = (x^3 + y^3) c^3(x^3, y^3).$$

Thus $(xa(x^3, y^3) : yb(x^3, y^3) : c(x^3 y^3)) \in \mathcal{V}$ and $\deg(xa(x^3, y^3)) = 3d' + 1$, so that in the language of Theorem 1.2(5), we have $(a, b, c) = (P, Q, R)$. □

The subject of equal sums of two cubes has a very long history. For example, the *Euler-Binet* formulas (see e.g. [5, §13.7]) give a complete parameterization to the equation

$$(4.9) \qquad\qquad X^3 + Y^3 = U^3 + V^3$$

over $\mathbb{Q}$, although an examination of the proof in [5] shows that it also applies to any field F of characteristic zero, such as $\mathbb{C}(x, y)$. The parameterization is:

$$(4.10) \quad \begin{aligned} X &= \lambda(1 - (a - 3b)(a^2 + 3b^2)), & Y &= \lambda((a + 3b)(a^2 + 3b^2) - 1), \\ U &= \lambda((a + 3b) - (a^2 + 3b^2)^2), & V &= \lambda((a^2 + 3b^2)^2 - (a - 3b)), \end{aligned}$$

where $a, b, \lambda \in F$. One can easily solve for (a, b, λ) for which $X = x, Y = y, U = f, V = g$, although the derivation assumes that $f^3 + g^3 = x^3 + y^3$, so it is unhelpful in finding solutions to (1.3). Further, these solutions do not necessarily come from simple choices of (a, b, λ). For example, in the case of (1.1), a computation shows that $(X, Y, U, V) = (x, y, f_4, g_4)$ arises (uniquely) from

$$(4.11) \qquad a = \frac{2x^2 + 5xy + 2y^2}{2(x^2 + xy + y^2)}, \quad b = -\frac{3xy(x + y)}{2(x^3 - y^3)}, \quad \lambda = -\frac{(x - y)^3}{9xy}.$$

If (g_4, f_4) is taken instead of (f_4, g_4), then a is a quotient of two quartics, b is a quotient of two quintics and λ is a quintic divided by a quartic.

Finally, we look at some more general sums of two cubes. If $h, k, F \in \mathbb{C}(x, y)$, $h^3 + k^3 = F$, $w = (h, k)$ and $v = (f, g) \in \mathcal{V}$, then there is (at least) a one-sided composition on all solutions to $X^3 + Y^3 = F$, given by $v \circ w = (f(h, k), g(h, k))$. This follows from

$$(4.12) \qquad\qquad f^3(h, k) + g^3(h, k) = h^3 + k^3 = F.$$

For example, with $F(x, y) = 2x^6 - 2y^6$ and $\gamma = 2^{1/3}$,

$$(4.13) \qquad (x^2 + xy - y^2)^3 + (x^2 - xy - y^2)^3 = (\gamma x^2)^3 + (-\gamma y^2)^3 = 2x^6 - 2y^6.$$

However, there is clearly no $v = (f, g) \in \mathcal{V}$ so that $x^2 + xy - y^2 = f(\gamma x^2, -\gamma y^2)$. Moreover, there are other solutions to

$$(4.14) \qquad a^3(x, y) + b^3(x, y) = (2x^6 - 2y^6)c^3(x, y).$$

For example,

$$(4.15) \qquad a_0(x, y) = x^3 + \tfrac{i}{\sqrt{3}}y^3, \quad b_0(x, y) = x^3 - \tfrac{i}{\sqrt{3}}y^3, \quad c_0(x, y) = x,$$

(and $(a_0(y, x), b_0(y, x), -c_0(y, x)))$ do not arise from composition of either solution of (4.13) with $\mathcal{V}$. We look forward to finding the complete structure of the solutions to (4.14).

References

[1] B. C. Berndt, *Number Theory in the Spirit of Ramanujan*, Student Mathematical Library **34**, American Mathematical Society, Providence, RI, 2006, MR2246314 (2007f:11001).

[2] B. C. Berndt and R. A. Rankin, *Ramanujan; Letters and Commentary*, History of Mathematics **9**. American Mathematical Society, Providence, RI; London Mathematical Society, London, 1995, MR1353909 (97c:01034).

[3] L. E. Dickson, *History of the Theory of Numbers, vol II: Diophantine Analysis*, Carnegie Institute, Washington 1920, reprinted by Chelsea, New York, 1971, MR0245500 (39 #6807b).

[4] M. D. Hirschhorn, *Three classical results on representations of a number*, Seminaire Lotharingien, **B42f**, 1998.

[5] G. H. Hardy and E. M. Wright, *An introduction to the Theory of Numbers, Sixth edition, revised by D. R. Heath-Brown and J. H. Silverman*, Oxford University Press, Oxford, 2008, MR2445243 (2009i:11001).

[6] B. Reznick and J. Rouse, *Viete's Bolero*, in preparation.

[7] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York-Heidelberg, 1979, MR0551363 (81f:10023).

[8] J. H. Silverman, *Taxicabs and Sums of Two Cubes*, Amer. Math. Monthly, **100** (1993), 331-340, MR1209462 (93m:11025).

[9] J. H. Silverman, *The arithmetic of elliptic curves, Second edition*, Graduate Texts in Mathematics, **106**, Springer, Dordrecht, 2009, MR2514094 (2010i:11005).

[10] François Viète, *The Analytic Art: Nine studies in Algebra, Geometry and Trigonometry from the Opus Restitutae Mathematicae Analyseos, seu Algebrâ Novâ*, translated by T. Richard Witmer, The Kent State University Press, Kent, Ohio 1983, Reprinted by Dover Publications, Inc., Mineola, NY, 2006, MR0731262 (86b:01012).

[11] Frank de Zeeuw, *An elliptic surface of rank 15*, master's thesis, University of Groningen, 2006. Available at `http://irs.ub.rug.nl/dbi/47ea4d97b56fa`.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, URBANA, IL 61801
E-mail address: `reznick@math.uiuc.edu`

DEPARTMENT OF MATHEMATICS, WAKE FOREST UNIVERSITY, WINSTON-SALEM, NC 27109
E-mail address: `rouseja@wfu.edu`