SOME DIOPHANTINE EQUATIONS RELATED TO POSITIVE-RANK ELLIPTIC CURVES

GWYNETH MORELAND AND MICHAEL E. ZIEVE

ABSTRACT. We give conditions on the rational numbers a, b, c which imply that there are infinitely many triples (x, y, z) of rational numbers such that $x + y + z = a + b + c$ and $xyz = abc$. We do the same for the equations $x + y + z = a + b + c$ and $x^3 + y^3 + z^3 = a^3 + b^3 + c^3$. These results rely on exhibiting families of positive-rank elliptic curves.

1. INTRODUCTION

Several authors have studied the following question:

Question 1.1. *For which triples (a, b, c) of pairwise distinct rational numbers does the system of equations $x + y + z = a + b + c$, $xyz = abc$ have infinitely many solutions in rational numbers x, y, z?*

In 1989, Kelly [12] showed that this system has infinitely many rational solutions if a, b, c are positive and satisfy certain easy-to-check conditions. In 1996, Schinzel [22] adapted an argument of Mordell's [16] to give a different proof of Kelly's result in case $(a, b, c) = (1, 2, 3)$. Recently Zhang and Cai [25] extended Schinzel's proof to the case $(a, b, c) = (1, 2, n)$ for any integer $n \geq 3$. Our first goal is to answer Question 1.1 in the greatest possible generality. We obtain the following result:

Theorem 1.2. *Let a, b, c be pairwise distinct rational numbers such that, for every permutation (A, B, C) of (a, b, c), we have*

$$A(B - C)^3 \neq B(C - A)^3 \tag{1.3}$$

and

$$AB^2 + BC^2 + CA^2 \neq 3ABC. \tag{1.4}$$

Then there are infinitely many triples (x, y, z) of rational numbers such that $x + y + z = a + b + c$ and $xyz = abc$.

There are infinitely many triples (a, b, c) of pairwise distinct nonzero rational numbers such that $a(b-c)^3 = b(c-a)^3$; in fact we will exhibit all such

Date: 4 April 2013.

The first author thank Community High School for enabling her to work with the second author via the Community Resource program. The second author was partially supported by the NSF under grant DMS-1162181.

triples in Proposition 4.2. It seems unlikely that there is a simple numerical property of such a triple (a, b, c) which determines whether the system $x+y+z = a+b+c,\ xyz = abc$ has infinitely many solutions $(x, y, z) \in \mathbb{Q}^3$, since we will show that this question is the same as determining whether an associated elliptic curve E_{abc} over $\mathbb{Q}$ has positive rank. However, we suspect that this system of equations has infinitely many rational solutions for roughly half of all triples (a, b, c) of pairwise distinct nonzero rational numbers such that $a(b-c)^3 = b(c-a)^3$. We will provide numerical and heuristic evidence for this belief in Section 4. Similar remarks apply for triples (a, b, c) such that $ab^2 + bc^2 + ca^2 = 3abc$.

Our next result exhibits a situation in which (1.3) and (1.4) automatically hold:

Corollary 1.5. *Let a, b, c be pairwise distinct integers which are pairwise coprime. Then there are infinitely many triples (x, y, z) of rational numbers such that $x + y + z = a + b + c$ and $xyz = abc$.*

Kelly [12] gave conditions on a, b, c which ensure that the system of equations $x + y + z = a + b + c,\ xyz = abc$ has infinitely many *positive* rational solutions. We recover his result as a consequence of Theorem 1.2:

Corollary 1.6 (Kelly)**.** *Let a, b, c be pairwise distinct positive rational numbers such that (1.3) holds for every permutation (A, B, C) of (a, b, c). Then there are infinitely many triples (x, y, z) of positive rational numbers such that $x + y + z = a + b + c$ and $xyz = abc$.*

The analogue of Corollary 1.5 for positive solutions is as follows:

Corollary 1.7. *Let a, b, c be pairwise distinct positive integers which are pairwise coprime. Then there are infinitely many triples (x, y, z) of positive rational numbers such that $x + y + z = a + b + c$ and $xyz = abc$.*

We will also prove analogues of Theorem 1.2 and Corollary 1.6 for the pair of equations $x + y + z = a + b + c$ and $x^3 + y^3 + z^3 = a^3 + b^3 + c^3$. This system has been studied in the physics literature, in the contex of zeros of $6j$ Racah coefficients [5]. We will prove the following results.

Proposition 1.8. *Let a, b, c be pairwise distinct rational numbers such that, for every permutation (A, B, C) of (a, b, c), we have*

$$(A+B)(A-B)^3 \neq (B+C)(B-C)^3 \tag{1.9}$$

and

$$AB^2 + BC^2 + CA^2 \neq A^3 + B^3 + C^3. \tag{1.10}$$

Then there are infinitely many triples (x, y, z) of rational numbers such that $x + y + z = a + b + c$ and $x^3 + y^3 + z^3 = a^3 + b^3 + c^3$.

Proposition 1.11. *Let a, b, c be pairwise distinct positive rational numbers such that every permutation (A, B, C) of (a, b, c) satisfies (1.9). Then there are infinitely many triples (x, y, z) of positive rational numbers such that $x + y + z = a + b + c$ and $x^3 + y^3 + z^3 = a^3 + b^3 + c^3$.*

Several authors have proved special cases of our results. Besides the papers of Kelly [12], Schinzel [22], and Zhang–Cai [25] mentioned previously, we note that Ren and Yang [19] proved Proposition 1.11 in the special case that a, b and c are three consecutive positive integers. Our results contradict several results in the recent paper [20] by Sadek and El-Sissi. The discrepancy stems from a mistake in in the proof of [20, Prop. 2.6], where it is asserted that the twelve points P_{ij}, $2P_{ij}$ (with $i \neq j$) are all distinct from one another. That is not always true, for instance it is not true when $(a, b, c) = (3, 10, 24)$. As a consequence, [20, Prop. 2.6] and [20, Thm. 2.7] are false, and the proof of [20, Thm. 3.1] is not valid. We note, however, that the paper [20] contains interesting material despite this mistake, for instance it uses this circle of ideas to produce high-rank elliptic curves. For other recent work on related questions, see [21, 23, 24, 26].

This paper is organized as follows. After some preliminary work in the next section, we prove Theorem 1.2 in Section 3. Our proof crucially relies on Mazur's theorem on rational torsion subgroups of elliptic curves [15]. In Section 4 we prove Corollary 1.5 and discuss Question 1.1 in the cases where Theorem 1.2 does not apply. We prove Corollaries 1.6 and 1.7 in Section 5, and in the final Section 6 we prove Propositions 1.8 and 1.11.

2. From equal sums and products to ranks of elliptic curves

In this section we translate Question 1.1 to the question of determining which elliptic curves in a certain infinite family have positive rank. For any $a, b, c \in \mathbb{Q}$, we write $s := a + b + c$ and $p := abc$. Let E_{abc} be the curve in $\mathbb{P}^2$ whose affine equation is

$$v^2 = u^3 - \Big(\frac{s^4}{48} - \frac{sp}{2}\Big)u + \Big(\frac{s^6}{864} - \frac{s^3p}{24} + \frac{p^2}{4}\Big), \tag{2.1}$$

and let S_{abc} be the variety in $\mathbb{A}^3$ defined by $x + y + z = s$ and $xyz = p$. If $p = 0$ then the set of rational points $S_{abc}(\mathbb{Q})$ is infinite, consisting of all permutations of all triples $(x, s-x, 0)$ with $x \in \mathbb{Q}$. In the more difficult case that $p \neq 0$, we now give a precise connection between $S_{abc}(\mathbb{Q})$ and $E_{abc}(\mathbb{Q})$.

Lemma 2.2. *For $a, b, c \in \mathbb{Q}^*$, the set of rational points $E_{abc}(\mathbb{Q})$ contains*

$$I_{abc} := \left\{ \Big(\frac{s^2}{12}, \frac{p}{2}\Big), \Big(\frac{s^2}{12}, -\frac{p}{2}\Big), \mathcal{O} \right\},$$

where $\mathcal{O}$ is the point $(0 : 1 : 0)$ in $\mathbb{P}^2$. The function

$$\rho\colon (x, y, z) \mapsto \Big(-\frac{p}{y} + \frac{s^2}{12}, -\frac{p}{y}(x + \frac{y}{2} - \frac{s}{2})\Big)$$

defines a homeomorphism $\rho\colon S_{abc}(\mathbb{R}) \to E_{abc}(\mathbb{R}) \setminus I_{abc}$ whose restriction to $S_{abc}(\mathbb{Q})$ induces a bijection of $S_{abc}(\mathbb{Q})$ with $E_{abc}(\mathbb{Q}) \setminus I_{abc}$.

Proof. This can be verified via a straightforward computation, in which one also verifies that $\rho^{-1}((u,v))$ equals

$$\left(\frac{v+\frac{1}{2}su-\frac{1}{24}s^3+\frac{1}{2}p}{u-\frac{1}{12}s^2},\ \frac{-p}{u-\frac{1}{12}s^2},\ \frac{-v+\frac{1}{2}su-\frac{1}{24}s^3+\frac{1}{2}p}{u-\frac{1}{12}s^2}\right). \qquad \square$$

In order to analyze whether the curve E_{abc} has infinitely many rational points, we now compute its genus.

Lemma 2.3. *For $a,b,c\in\mathbb{Q}^*$, the curve E_{abc} has genus 0 if $(a+b+c)^3=27abc$, and has genus 1 otherwise.*

Proof. Since the affine equation for E_{abc} is a Weierstrass equation, it defines an irreducible curve of genus 0 or 1. Genus 0 occurs if and only if $\Delta=0$, where $\Delta:=p^3(s^2-27p)$ is the discriminant of the Weierstrass equation. $\square$

We conclude this section by addressing the genus zero cases. Our next result exhibits the triples (a,b,c) for which E_{abc} has genus 0.

Lemma 2.4. *If $a,b,c\in\mathbb{Q}^*$ satisfy $(a+b+c)^3=27abc$, and a,b,c are not all equal, then there is a unique $t\in\mathbb{Q}\setminus\{0,1\}$ such that*

$$a=c(t-1)^3 \quad \text{and} \quad b=-ct^3.$$

Conversely, for any $c,t\in\mathbb{Q}^*$ with $t\neq 1$, the above equations define elements $a,b\in\mathbb{Q}^*$ such that $(a+b+c)^3=27abc$ and a,b,c are not all equal; moreover, a,b,c are pairwise distinct if and only if $t\notin\{-1,\frac{1}{2},2\}$.

Proof. It is straightforward to verify the final sentence in the result. Now fix $a,b,c\in\mathbb{Q}^*$ such that $(a+b+c)^3=27abc$, where a,b,c are not all equal. If $t\in\mathbb{Q}^*$ satisfies $a=r(t-1)^3$ and $b=-rt^3$, then $t^3=-b/c$, so there is at most one choice for t. It remains only to show that there exists $t\in\mathbb{Q}\setminus\{0,1\}$ such that $a=r(t-1)^3$ and $b=-rt^3$. We will show that these equations are satisfied for $t=(-a+2b-c)/(a+b-2c)$. First, note that $a+b\neq 2c$: for, if $a+b=2c$ then $(3c)^3=(a+b+c)^3=27abc$ implies $c^2=ab$, so that $(a-b)^2=(a+b)^2-4ab=(2c)^2-4c=0$, which gives the contradiction $a=b=(a+b)/2=c$. Now it is straightforward to check that

$$a-c(t-1)^3=\frac{(a-c)((a+b+c)^3-27abc)}{c(a+b-2c)^3}$$
$$b+ct^3=\frac{(b-c)((a+b+c)^3-27abc)}{c(a+b-2c)^3},$$

so that indeed $a=c(t-1)^3$ and $b=-ct^3$. Next we show that our specified value of t is neither 0 nor 1. For, if $t=0$ then $a+c=2b$, and if $t=1$ then $b+c=2a$; either of these implies $a=b=c$ via the same argument we used to show that $a+b\neq 2c$. This completes the proof. $\square$

Finally, we determine $S_{abc}(\mathbb{Q})$ when E_{abc} has genus zero.

Lemma 2.5. *For any $c \in \mathbb{Q}^*$ and $t \in \mathbb{Q} \setminus \{-1, 0, \frac{1}{2}, 1, 2\}$, put $a = c(t-1)^3$ and $b = -ct^3$. Then $S_{abc}(\mathbb{Q}) \setminus \{c(t-t^2), c(t-t^2), c(t-t^2))\}$ equals*

$$\left\{ \Big(\frac{ct(t-1)^3}{(u+1)(u+t)}, -\frac{ct(u+t)^2}{u+1}, \frac{ct(u+1)^2}{u+t} \Big) : u \in \mathbb{Q} \setminus \{-1, -t\} \right\}.$$

Proof. Fix $c \in \mathbb{Q}^*$ and $t \in \mathbb{Q} \setminus \{-1, 0, \frac{1}{2}, 1, 2\}$, and put $a = c(t-1)^3$ and $b = -ct^3$. For $A = a/c$ and $B = b/c$, the set $S_{abc}(\mathbb{Q})$ is obtained from $S_{AB1}(\mathbb{Q})$ by multiplying all coordinates of all points by c. Hence it suffices to prove the result in case $c = 1$, and to simplify the notation we will assume $c = 1$ in what follows. For any $u \in \mathbb{Q} \setminus \{-1, -t\}$, one easily checks that

$$P_u := \Big(\frac{t(t-1)^3}{(u+1)(u+t)}, -\frac{t(u+t)^2}{u+1}, \frac{t(u+1)^2}{u+t} \Big)$$

is in $S_{abc}(\mathbb{Q})$. We have $P_u \neq (t-t^2, t-t^2, t-t^2)$, since otherwise by equating x-coordinates we would obtain $(t-1)^2 + (u+1)(u+t) = 0$, which is a quadratic polynomial in u whose discriminant is the nonsquare $-3(t-1)^2$. Now let (x, y, z) be any point in $S_{abc}(\mathbb{Q})$ which does not equal either (a, b, c) or $(t-t^2, t-t^2, t-t^2)$. Since $P_0 = (a, b, c)$, it suffices to prove that $(x, y, z) = P_u$ for some $u \in \mathbb{Q} \setminus \{-1, -t\}$. We will prove this for the value

$$u := -\frac{2t^4 + t^3 z - 2t^3 + tyz + ty - yz}{t(t^3 + tz - t + y)}.$$

We first check that this expression for u defines a rational number, by showing that its denominator is nonzero. If $y = -t^3 - tz + t$ then $x = a + b + c - y - z = (t-1)(z + t^2 - 2t)$, so $-t^3(t-1)^3 = abc = xyz = (t-1)(z+t^2-2t)(-t^3-tz+t)z$, or equivalently $t(t-1)(z-1)(z+t^2-t)^2 = 0$; thus either $z = 1$ or $z = t - t^2$, which imply that (x, y, z) is either (a, b, c) or $(t - t^2, t - t^2, t - t^2)$, contradicting our hypothesis. Next we check that $u \neq -1$: for, otherwise we would obtain $y = -t^2 + (t^2 - t^3)z^{-1}$, so $x = a + b + c - y - z = -z + (3t - 2t^2) + (t^3 - t^2)z^{-1}$ and the equation $xyz = abc$ implies that $z \in \{1, t - t^2\}$, which again gives the contradiction $(x, y, z) \in \{((t-1)^3, -t^3, 1), (t - t^2, t - t^2, t - t^2)\}$. The same reasoning shows that $u \neq -t$: for, if $u = -t$ then $z = t + (t^4 - t^3)y^{-1}$, so from $x + y + z = a + b + c$ and $xyz = abc$ we obtain $y \in \{-t^3, t - t^2\}$, giving the same contradiction as above. Writing $P_u = (\hat{x}, \hat{y}, \hat{z})$, one can check that

$$\begin{aligned}
\hat{x} - x &= -\frac{(xyz - abc)(yz - ty + t^2 z - t^4 + t^3 - t^2)}{(yz + t^2 z + t^3 - t^2)(yz - ty - t^4 + t^3)}, \\
\hat{y} - y &= \frac{(xyz - abc)(y + t^3)}{(y + tz + t^3 - t)(yz + t^2 z + t^3 - t^2)}, \quad \text{and} \\
\hat{z} - z &= \frac{t(xyz - abc)(z - 1)}{(y + tz + t^3 - t)(yz - ty - t^4 + t^3)},
\end{aligned}$$

so that $(x, y, z) = (\hat{x}, \hat{y}, \hat{z}) = P_u$, which completes the proof. □

3. Positive-rank elliptic curves

In this section we prove Theorem 1.2, by showing that certain elliptic curves have positve rank. Our proof relies on Mazur's theorem on rational torsion of elliptic curves [15]:

Theorem 3.1 (Mazur)**.** *For any elliptic curve E over $\mathbb{Q}$, the torsion subgroup of $E(\mathbb{Q})$ is isomorphic to either $\mathbb{Z}/n\mathbb{Z}$ (with $1 \le n \le 12$ and $n \ne 11$) or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ (with $1 \le n \le 4$).*

Recall that, for any $a, b, c \in \mathbb{Q}$, the set $S_{abc}(\mathbb{Q})$ consists of all triples (x, y, z) of rational numbers such that $x + y + z = a + b + c$ and $xyz = abc$. Also, E_{abc} is the curve in $\mathbb{P}^2$ defined by the affine equation (2.1). Finally, we write Σ_{abc} for the set of permutations of the sequence (a, b, c). We will prove the following refinement of Theorem 1.2:

Theorem 3.2. *Let a, b, c be pairwise distinct nonzero rational numbers. If $(a + b + c)^3 = 27abc$ then E_{abc} has genus zero and $S_{abc}(\mathbb{Q})$ is infinite. If $(a+b+c)^3 \ne 27abc$ then E_{abc} is an elliptic curve which contains the points in the set*

$$T_{abc} := \left\{ \left(-AC + \frac{(A+B+C)^2}{12}, \frac{AC(C-A)}{2} \right) : (A, B, C) \in \Sigma_{abc} \right\},$$

and the subgroup of $E_{abc}(\mathbb{Q})$ generated by T_{abc} is

$$\begin{cases} \mathbb{Z}/12\mathbb{Z} & \text{if } A(B-C)^3 = B(C-A)^3 \text{ for some } (A,B,C) \in \Sigma_{abc}, \\ \mathbb{Z}/9\mathbb{Z} & \text{if } AB^2 + BC^2 + CA^2 = 3ABC \text{ for some } (A,B,C) \in \Sigma_{abc}, \\ \mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \text{otherwise.} \end{cases}$$

In light of Lemma 2.2, Theorem 1.2 follows at once from Theorem 3.2 and the fact that $S_{abc}(\mathbb{Q})$ is infinite when $abc = 0$. We now prove Theorem 3.2.

Proof of Theorem 3.2. Let a, b, c be pairwise distinct nonzero rational numbers. By Lemmas 2.4 and 2.5, the set $S_{abc}(\mathbb{Q})$ is infinite if $(a+b+c)^3 = 27abc$, and Lemma 2.3 implies that E_{abc} has genus zero in this case. Henceforth assume that $(a + b + c)^3 \ne 27abc$, so that (by Lemma 2.3) the curve E_{abc} is an elliptic curve. Lemma 2.2 implies that $E_{abc}(\mathbb{Q})$ contains T_{abc}. For any permutation (A, B, C) of (a, b, c), write

$$P_{ABC} := \left(-AC + \frac{(A+B+C)^2}{12}, \frac{AC(C-A)}{2} \right).$$

Then, in the group $E_{abc}(\mathbb{Q})$, we have the relations $P_{CBA} = -P_{ABC}$ and $P_{CAB} = P_{ABC} + Q$, where $Q := ((a + b + c)^2/12, abc/2)$. Crucially, we observe that Q has order 3. Writing Γ_{abc} for the group generated by T_{abc}, it follows that $\Gamma_{abc} = \langle P_{ABC}, Q \rangle$ for any $(A, B, C) \in \Sigma_{abc}$. In particular, if Γ_{abc} is infinite then $\Gamma_{abc} \cong \mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Note that $P_{ABC} \ne P_{DEF}$ for any distinct $(A, B, C), (D, E, F) \in \Sigma_{abc}$, since if P_{ABC} and P_{DEF} have the same x-coordinate then $AC = DF$ so $B = E$, whence $P_{DEF} = P_{CBA} = -P_{ABC} \ne P_{ABC}$. Next, considering x-coordinates shows that the group $\langle Q \rangle$ is disjoint

from T_{abc}, so $\#\Gamma_{abc} \geq 9$. By Mazur's theorem, if Γ_{abc} is finite then it must be either $\mathbb{Z}/9Z$, $\mathbb{Z}/12\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$; in any case, Γ_{abc} has a unique subgroup of order 3. For any $(A, B, C) \in \Sigma_{abc}$, we compute that $2P_{ABC}$ equals

$$\Big(\frac{(A+B+C)^2}{12} - \frac{AC(A-B)(B-C)}{(A-C)^2},\ \frac{AC}{2(A-C)^3}(A(C-B)^3 - C(B-A)^3)\Big).$$

Examining x-coordinates shows that $2P_{ABC} \notin \langle Q \rangle$, so the order of P_{ABC} does not divide 6. It follows that $\Gamma_{abc} \ncong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

We now determine all a, b, c for which $\Gamma_{abc} \cong \mathbb{Z}/12\mathbb{Z}$. First note that this occurs if and only if some P_{ABC} has order 4: for, if P_{ABC} has order 4 then $\Gamma_{abc} = \langle P_{ABC}, Q \rangle \cong \mathbb{Z}/12\mathbb{Z}$, and if $\Gamma_{abc} \cong \mathbb{Z}/12\mathbb{Z}$ then some element of T_{abc} has order 4 because $\mathbb{Z}/12\mathbb{Z}$ contains only four elements whose order is neither 4 nor a divisor of 6. Next, P_{ABC} has order 4 if and only if $2P_{ABC}$ has order 2; equivalently, the y-coordinate of $2P_{ABC}$ is zero, which means that $A(C-B)^3 = C(B-A)^3$.

Finally, we determine all a, b, c for which $\Gamma_{abc} \cong \mathbb{Z}/9\mathbb{Z}$. This occurs if and only if every P_{ABC} has order 9, which means that $3P_{ABC} = \pm Q$. Since $P_{CBA} = -P_{ABC}$, this says that some P_{ABC} satisfies $3P_{ABC} = Q$, or equivalently $2P_{ABC} = -P_{ABC} + Q$. We compute

$$-P_{ABC} + Q = \Big(\frac{(A+B+C)^2}{12} - AB,\ \frac{1}{2}AB(B-A)\Big).$$

Note that $2P_{ABC} \neq -(-P_{ABC} + Q)$, since $P_{ABC} \neq Q$. Thus, $-P_{ABC} + Q$ and $2P_{ABC}$ are equal if and only if they have the same x-coordinate, which says that

$$B(A-C)^2 = C(A-B)(B-C),$$

or equivalently

$$A^2B + B^2C + C^2A = 3ABC. \qquad \square$$

4. The remaining cases of Question 1.1

In this section we discuss Question 1.1 in the cases where either (1.3) or (1.4) does not hold. We first show that (1.3) and (1.4) automatically hold in certain situations, and use this to prove Corollary 1.5.

Lemma 4.1. *If a, b, c are nonzero integers which are pairwise coprime and pairwise distinct, then $a(b-c)^3 \neq b(c-a)^3$ and $ab^2 + bc^2 + ca^2 \neq 3abc$.*

Proof. First assume that $a(b-c)^3 = b(c-a)^3$, so $a \mid b(c-a)^3$. Since a is coprime to b and c, it is coprime to $b(c-a)^3$, so $a \in \{-1, 1\}$. Likewise, $b \in \{1, -1\}$, so $b = -a$. Then $a(b-c)^3 = b(c-a)^3 = a(a-c)^3$, so that $b - c = a - c$ and thus $b = a$, a contradiction.

Next assume that $ab^2 + bc^2 + ca^2 = 3abc$. Then $a \mid bc^2$, and since a is coprime to b and c, it follows that $a \in \{1, -1\}$. Likewise, both b and c must be in $\{1, -1\}$, so a, b, c cannot be pairwise distinct. $\square$

Corollary 1.5 follows at once from this result and Theorem 1.2, together with the fact that (1.3) and (1.4) hold for every permutation (A, B, C) of $(-1, 0, 1)$.

Next we determine all (a, b, c) for which either (1.3) or (1.4) does not hold.

Proposition 4.2. *The triples (a, b, c) of pairwise distinct nonzero rational numbers such that $a(b-c)^3 = b(c-a)^3$ are*

$$(r(t+1)^3,\ -rt^3,\ -rt(t+1)(2t^2+2t+1))$$

where $r \in \mathbb{Q}^*$ and $t \in \mathbb{Q}\setminus\{-1, -\frac{1}{2}, 0\}$. The triples (a, b, c) of pairwise distinct nonzero rational numbers such that $ab^2 + bc^2 + ca^2 = 3abc$ are

$$(rt^2,\ -r(t+1),\ rt(t+1)^2)$$

where $r \in \mathbb{Q}^*$ and $t \in \mathbb{Q} \setminus \{-1, 0\}$. In both cases, the pair (r, t) is uniquely determined by the triple (a, b, c).

Proof. Let a, b, c be pairwise distinct nonzero rational numbers such that $a(b-c)^3 = b(c-a)^3$. Then $t := (b-c)/(a-b)$ is a nonzero rational number. Further, $t \neq -1$ since otherwise $b - c = b - a$ implies $a = c$. Finally, $t \neq -\frac{1}{2}$, since otherwise $2(b-c) = b-a$ implies $b-c = c-a$, so the identity $a(b-c)^3 = b(c-a)^3$ reduces to $a = b$. Thus $t \in \mathbb{Q} \setminus \{-1, -\frac{1}{2}, 0\}$, and for $r := a/(t+1)^3$ we compute

$$b + rt^3 = \frac{a(b-c)^3 - b(c-a)^3}{(a-c)^3}$$

and

$$c + rt(t+1)(2t^2+2t+1) = \frac{a(b-c)^3 - b(c-a)^3}{(a-b)(a-c)^2},$$

so $(a, b, c) = (r(t+1)^3,\ -rt^3,\ -rt(t+1)(2t^2+2t+1))$. Conversely, this last equation implies that $ab^{-1} = -(1+t^{-1})^3$, so that t (and hence r) is uniquely determined by a and b; moreover, for any $r \in \mathbb{Q}^*$ and $t \in \mathbb{Q} \setminus \{-1, -\frac{1}{2}, 0\}$, if we define a, b, c by this last equation then $a, b, c \in \mathbb{Q}^*$ are pairwise distinct and $a(b-c)^3 = b(c-a)^3$.

Now let a, b, c be pairwise distinct nonzero rational numbers such that $ab^2 + bc^2 + ca^2 = 3abc$. Then $t := (a-c)/(b-a)$ is a nonzero rational number, and $t \neq -1$ since $b \neq c$. For $r := a/t^2$ we compute

$$b + r(t+1) = \frac{ab^2 + bc^2 + ca^2 - 3abc}{(a-c)^2}$$

and

$$c - rt(t+1)^2 = \frac{ab^2 + bc^2 + ca^2 - 3abc}{(a-b)(a-c)},$$

so $(a, b, c) = (rt^2,\ -r(t+1),\ rt(t+1)^2)$. Conversely, this last equation implies that $acb^{-2} = t^3$, so that t (and hence r) is uniquely determined by (a, b, c); moreover, for any $r \in \mathbb{Q}^*$ and any $t \in \mathbb{Q} \setminus \{-1, 0\}$, if we define a, b, c by this last equation then $a, b, c \in \mathbb{Q}^*$ are pairwise distinct and $ab^2 + bc^2 + ca^2 = 3abc$. □

Next we show that the failure of (1.3) or (1.4) does not determine whether $S_{abc}(\mathbb{Q})$ is infinite.

Example 4.3. One can check that $E_{abc}(\mathbb{Q})$ is finite when (a,b,c) is either $(3,10,24)$ or $(1,-2,4)$, and infinite when (a,b,c) is either $(2,15,54)$ or $(-3,4,18)$. Here $(a,b,c) = (3,24,10)$ and $(2,54,15)$ violate (1.3), but every permutation (A,B,C) of either of these triples satisfies (1.4). On the other hand, $(a,b,c) = (1,-2,4)$ and $(-3,18,4)$ violate (1.4), but every permutation (A,B,C) of either of these triples satisfies (1.3).

In the spirit of existing conjectures (e.g. from [1]), and in the absence of any reason to believe otherwise, it seems reasonable to guess that $S_{abc}(\mathbb{Q})$ is infinite for half of all triples (a,b,c) of nonzero rational numbers such that either $a(b-c)^3 = b(c-a)^3$ or $ab^2+bc^2+ca^2 = 3abc$, when triples are ordered by the largest absolute value of any integer occurring as either a numerator or denominator of any rational number in the triple. We used Magma's non-rigorous calculation of analytic ranks of elliptic curves to compute the analytic rank of E_{abc} for all triples (a,b,c) of nonzero pairwise coprime rational numbers which violate either (1.3) or (1.4) and whose numerator and denominator have absolute value at most 30. There are 1801 such triples, and Magma suggests that the analytic rank of E_{abc} is zero for 783 (or about 43.48%) of them. By Lemma 2.2 and the Birch–Swinnerton-Dyer conjecture, the analytic rank of E_{abc} is zero precisely when $S_{abc}(\mathbb{Q})$ is finite. If we so desire, we can avoid assuming the Birch–Swinnerton-Dyer conjecture here by restricting to cases where the analytic rank of E_{abc} is at most one, since the Birch–Swinnerton-Dyer conjecture is known to be true in those cases by results of Gross–Zagier [10] and Kolyvagin [13], together with [4] and either [6] or [17]. Although 43.48% is somewhat less than 50%, it is closer to 50% than is usual for data involving ranks of elliptic curves, so at least we can say that our guess is more consistent with the data than are well-established conjectures of the same flavor [1].

5. Positive solutions

In this section we examine positive rational solutions of the system $x+y+z = a+b+c$, $xyz = abc$. We will use the Poincaré–Hurwitz theorem ([11, Satz 13]; see also [18, p. 173]):

Lemma 5.1 (Poincaré–Hurwitz)**.** *Let E be a nonsingular cubic curve in $\mathbb{P}^2$ which is defined over/ $\mathbb{Q}$. If the set $E(\mathbb{Q})$ is infinite, then every open subset of $\mathbb{P}^2(\mathbb{R})$ which contains one point of $E(\mathbb{Q})$ must contain infinitely many points of $E(\mathbb{Q})$.*

We now prove a refined version of Corollary 1.6, which will be needed in the next section.

Lemma 5.2. *Let a,b,c be pairwise distinct positive rational numbers such that every permutation (A,B,C) of (a,b,c) satisfies $A(B-C)^3 \neq B(C-A)^3$.*

Then $S_{abc}(\mathbb{Q})$ contains infinitely many points in any open subset of $\mathbb{R}^3$ which contains (a,b,c).

Proof. Since a,b,c are distinct and positive, their arithmetic mean is greater than their geometric mean, so $(a+b+c)^3 > 27abc$. Likewise, for any permutation (A,B,C) of (a,b,c), comparing the arithmetic and geometric means of AB^2, BC^2 and CA^2 shows that $AB^2+BC^2+CA^2 \geq 3ABC$, with equality occurring if and only if $AB^2 = BC^2 = CA^2$. This equality condition implies that $A^2B^4 = (AB^2)^2 = (BC^2)(CA^2) = A^2BC^3$, so that $B^3 = C^3$, which is impossible since B, C are distinct rational numbers. Thus, Theorem 3.2 tells us that E_{abc} is an elliptic curve containing infinitely many rational points, so by Lemma 5.1 the set $E_{abc}(\mathbb{Q})$ has infinite intersection with any neighborhood in $\mathbb{P}^2(\mathbb{R})$ of any point $P \in E_{abc}(\mathbb{Q})$. Since the map ρ from Lemma 2.2 is a homeomorphism from $S_{abc}(\mathbb{R})$ to $E_{abc}(\mathbb{R}) \setminus I_{abc}$, it follows that $S_{abc}(\mathbb{Q})$ has infinite intersection with any neighborhood in $\mathbb{R}^3$ of $\rho^{-1}(P)$ if $P \notin I_{abc}$. Taking $P = \rho((a,b,c))$ yields the result. □

Corollary 1.6 follows from Lemma 5.2 by taking the open set to be an open ball centered at (a,b,c) of radius less than the smallest of a,b,c. Next, Corollary 1.7 follows at once from Corollary 1.6 and Lemma 4.1.

6. Equal sums and equal sums of cubes

In this section we analyze the system of equations $x+y+z = a+b+c$, $x^3+y^3+z^3 = a^3+b^3+c^3$ for fixed $a,b,c \in \mathbb{Q}$. This system has been studied at least since 1915 [9], and more recently in the papers [2, 3, 5, 7, 8, 14, 19], inspired in part by the occurrence of this system in the physics literature in the context of zeros of the $6j$ Racah coefficients [5].

We use a substitution from [5] (in slightly modified form) to transform this system into the system $u+v+w = d+e+f$, $uvw = def$ for certain $d,e,f \in \mathbb{Q}$. For any field K with $\mathrm{char}(K) \neq 2$, define $\psi\colon K^3 \to K^3$ and $\phi\colon K^3 \to K^3$ via

$$\psi((x,y,z)) = \Big(\frac{y+z}{2}, \frac{x+z}{2}, \frac{x+y}{2}\Big)$$
$$\phi((x,y,z)) = (-x+y+z,\ x-y+z,\ x+y-z).$$

For fixed $a,b,c \in \mathbb{Q}$, let U_{abc} be the variety defined by $x+y+z = a+b+c$ and $x^3+y^3+z^3 = a^3+b^3+c^3$.

Lemma 6.1. *The functions ψ and ϕ are bijective and inverse to one another. For any $a,b,c \in \mathbb{Q}$, we have $U_{abc}(K) = \phi(S_{\psi((a,b,c))}(K))$ and $S_{abc}(K) = \psi(U_{\phi((a,b,c))}(K))$.*

Proof. It is easy to check that both $\phi\circ\psi$ and $\psi\circ\phi$ are the identity map on K^3, which implies that they are inverses and they are both bijective. Letting $s\colon K^3 \to K$ be the map $s((x,y,z)) = x+y+z$, we see that $s\circ\phi = s = s\circ\psi$. Pick any $a,b,c,x,y,z \in K$ such that $x+y+z = a+b+c$. Let $(u,v,w) =$

$\psi((x,y,z))$ and $(d,e,f) = \psi((a,b,c))$, so that also $(x,y,z) = \phi((u,v,w))$ and $(a,b,c) = \phi((d,e,f))$. Then we have

$$x^3+y^3+z^3 = (-u+v+w)^3+(u-v+w)^3+(u+v-w)^3 = (u+v+w)^3-24uvw,$$

and likewise $a^3+b^3+c^3 = (d+e+f)^3-24def$. Since

$$u+v+w = x+y+z = a+b+c = d+e+f,$$

it follows that $x^3+y^3+z^3$ and $a^3+b^3+c^3$ are equal if and only if uvw and def are equal. Thus $U_{abc}(K) = \phi(S_{def}(K))$ and $S_{def}(K) = \psi(U_{abc}(K))$. □

We conclude this paper with proofs of Propositions 1.8 and 1.11.

Proof of Proposition 1.8. Write $(d,e,f) := \psi((a,b,c))$, so that Lemma 6.1 exhibits a bijection between $U_{abc}(\mathbb{Q})$ and $S_{def}(\mathbb{Q})$. Since a,b,c are pairwise distinct, also d,e,f are pairwise distinct. By Theorem 1.2, the set $S_{def}(\mathbb{Q})$ is infinite so long as every permutation (D,E,F) of (d,e,f) satisfies both $D(E-F)^3 \neq E(F-D)^3$ and $DE^2+EF^2+FD^2 \neq 3DEF$. These hypotheses are equivalent to the assertion that (1.9) and (1.10) hold for every permutation (A,B,C) of (a,b,c), so the result follows. □

Proof of Proposition 1.11. Write $(d,e,f) := \psi((a,b,c))$, so d,e,f are pairwise distinct positive rational numbers. Our hypothesis on a,b,c implies that $D(E-F)^3 \neq E(F-D)^3$ for every permutation (D,E,F) of (d,e,f). Thus, by Lemma 5.2, the set $S_{def}(\mathbb{Q})$ contains infinitely many points in any open subset of $\mathbb{R}^3$ which contains (d,e,f). Since ϕ is a homeomorphism from $\mathbb{R}^3$ to itself, and $(a,b,c) = \phi((d,e,f))$ is in $\phi(S_{def}(\mathbb{Q}))$, it follows that $\phi(S_{def}(\mathbb{Q}))$ contains infinitely many points in any open subset of $\mathbb{R}^3$ which contains (a,b,c). Finally, Lemma 6.1 shows that $\phi(S_{def}(\mathbb{Q})) = U_{abc}(\mathbb{Q})$, so the result follows by choosing the open set to be an open ball centered at (a,b,c) of radius less than the smallest of a,b,c. □

References

[1] B. Bektemirov, B. Mazur, W. Stein and M. Watkins, *Average ranks of elliptic curves: tension between data and conjecture*, Bull. Amer. Math. Soc. **44** (2007), 233–254. 9

[2] A. Bremner, *Diophantine equations and nontrivial Racah coefficients*, J. Math. Phys. **27** (1986), 1181–1184. 10

[3] A. Bremner and S. Brudno, *A complete determination of the zeros of weight-1 6j coeffiicients*, J. Math. Phys. **27** (1986), 2613–2615. 10

[4] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939. 9

[5] S. Brudno and J. D. Louck, *Nontrivial zeros of weight 1 3j and 6j coefficients: Relation to diophantine equations of equal sums of like powers*, J. Math. Phys. **26** (1985), 2092–2095. 2, 10

[6] D. Bump, S. Friedberg and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), 543–618. 9

[7] A. Choudhry, *Symmetric diophantine systems*, Acta Arith. **59** (1991), 291–307. 10
[8] A. Choudhry, *Some diophantine problems concerning equal sums of integers and their cubes*, Hardy–Ramanujan J. **33** (2010), 59–70. 10
[9] A. Gérardin, L'intermédiaire des math. **22** (1915), 130–132. 10
[10] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320. 9
[11] A. Hurwitz, *Über ternäre diophantische Gleichungen dritten Grades*, Vierteljahrsschr. Naturf. Ges. Zürich **62** (1917), 207–229. 9
[12] J. B. Kelly, *Partitions with equal products (II)*, Proc. Amer. Math. Soc. **107** (1989), 887–893. 1, 2, 3
[13] V. A. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* $Ш(E,\mathbb{Q})$ *for a subclass of Weil curves*, Math. USSR-Izv. **32** (1989), 523–541. 9
[14] J. J. Labarthe, *Parametrization of the linear zeros of* $6j$ *coefficients*, J. Math. Phys. **27** (1986), 2964–2965. 10
[15] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.E.S. **47** (1977), 33–186. 3, 6
[16] L. J. Mordell, *Rational quadrilaterals*, J. London Math. Soc. **35** (1960), 277–282. 1
[17] M. R. Murty and V. K. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. (2) **133** (1991), 447–475. 9
[18] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques*, J. Math. Pures Appl. (5) **7** (1901), 161–233. 9
[19] R. Ren and D. Yang, *A Diophantine problem from mathematical physics*, preprint, 2012. 3, 10
[20] M. Sadek and N. El-Sissi, *Partitions with equal products and elliptic curves*, arXiv:1303.6705v1, 26 Mar 2013. 3
[21] M. Satriano, Z. Scherr and M. E. Zieve, *Complete reducibility of polynomials with varying coefficients*, preprint. 3
[22] A. Schinzel, *Triples of positive integers with the same sum and the same product*, Serdica Math. J. **22** (1996), 587–588. 1, 3
[23] M. Ulas, *On some Diophantine systems involving symmetric polynomials*, Math. Comp., to appear. 3
[24] Y. Zhang and T. Cai, *n-tuples of positive integers with the same second elementary symmetric function value and the same product*, J. Number Theory **132** (2012), 2065–2074. 3
[25] Y. Zhang and T. Cai, *n-tuples of positive integers with the same sum and the same product*, Math. Comp. **82** (2013), 617–623. 1, 3
[26] M. E. Zieve, *A remark on the paper "N-tuples of positive integers with the same sum and the same product" by Zhang and Cai*, Math. Comp., to appear. 3

Community High School, Ann Arbor, MI 48104, USA
E-mail address: gwynsm@gmail.com

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109–1043, USA
E-mail address: zieve@umich.edu
URL: www.math.lsa.umich.edu/∼zieve/