Stud. Univ. Babeş-Bolyai Math. 64(2019), No. 3, 349–356
DOI: http://dx.doi.org/10.24193/subbmath.2019.3.06

An elliptic Diophantine equation from the study of partitions

Dorin Andrica and George C. Ţurcaş

Abstract. We present the elliptic equation $X^3+2=Y^2$ as the first in a sequence of Diophantine equations arising from some new results in the theory of partitions of multisets with equal sums. Two proofs for Theorem 2.3, showing that the only integer solutions to this equation are $(-1,1)$ and $(-1,-1)$, are given.

Mathematics Subject Classification (2010): 14G05, 11P57, 11Y50.

Keywords: Elliptic curves, partitions of a set, Mordell equations, Lutz-Nagell theorem.

1. Introduction and motivation

For a positive integer $k\geq 2$ and an arbitrary positive integer n, in the papers [2] and [1] the authors introduced the sequence $(Q_k(n))_{n\geq 1}$,

$$Q_k(n)=\frac{1}{2\pi}\int_0^{2\pi}\prod_{s=1}^{n}(k-2+2\cos st)\,\mathrm{d}t. \tag{1.1}$$

An enumerative formula for $Q_k(n)$ is given by the number of ordered partitions of $[n]=\{1,\ldots,n\}$ into k disjoint sets $A_1,\ldots,A_k$ with the property that $\sigma(A_1)=\sigma(A_k)$, where $\sigma(A)$ denotes the sum of all elements in A.

Clearly, $Q_k(n)$ is a monic polynomial of degree n in $k-2$. Moreover, in the paper [2] is proved that

$$Q_k(n)=\sum_{d=0}^{n}N(d,n)(k-2)^{n-d}, \tag{1.2}$$

where for each $d=0,\ldots,n$, the coefficient $N(d,n)$ is the number of ordered partitions of $[n]$ into 3 subsets A,B,C such that $|B|=d$ and $\sigma(A)=\sigma(C)$, where $|B|$ is the cardinality of B.

Therefore, $Q_k(n)$ has non-negative integer coefficients, and each coefficient has a combinatorial meaning in terms of partitions of the set $[n]$. A simple direct computation of the

The second author is supported by an EPSRC PhD studentship.

integral (1.1) shows that for $n = 3, 4, 5, 6$ and $k \geq 2$, we have

$$Q_k(3) = (k-2)^3 + 2;$$
$$Q_k(4) = (k-2)^4 + 4(k-2) + 2;$$
$$Q_k(5) = (k-2)^5 + 8(k-2)^2 + 6(k-2);$$
$$Q_k(6) = (k-2)^6 + 12(k-2)^3 + 16(k-2)^2 + 6(k-2).$$

The sequence $Q_k(3)$ is indexed as A084380 in OEIS [10], where it is mentioned that it does not contain any perfect squares, i.e. the elliptic equation $X^3 + 2 = Y^2$ has no solutions in positive integers. This is linked to a Catalan-type conjecture related to Pillai's equation $X^U - Y^V = m$, with $X, Y, U, V \geq 2$ integers. The conjecture states that for any given integer m, there are finitely many perfect powers whose difference is m (see [13], Conjecture 1.6). For $m = 2$, it was computationally checked that the only solution involving perfect powers smaller than 10^{18} is $2 = 3^3 - 5^2$. The number of such solutions is linked to A076427 in OEIS.

Motivated by the property that the sequence $Q_k(3)$ does not contain any perfect squares, in the papers [2] and [1], the authors suggested the following problems: study if the sequence $Q_k(n)$ contains any $n-1$ powers, where $n = 4, 5$ or 6. These are equivalent to the study of the following Diophantine equations:

$$X^4 + 4X + 2 = Y^3;$$
$$X^5 + 8X^2 + 6X = Y^4;$$
$$X^6 + 12X^3 + 16X^2 + 6X = Y^5.$$

Using effective methods for identifying integral points on curves, we will discuss these equations and variations of them in a following series of papers.

In Theorem 2.3 of the present paper we prove that the equation $X^3 + 2 = Y^2$ has only integer solutions $(-1, 1)$ and $(-1, -1)$. We give two proofs for this statement. In the first we use the fact that $\mathbb{Q}(\sqrt{2})$ has trivial class group, property that allows us to pass from factorisations of ideals to nice factorisations in the ring $\mathbb{Z}[\sqrt{2}]$. The second proof uses the geometry of the elliptic curve defining the equation.

2. The equation $Y^2 = X^3 + 2$

Although the family of Mordell equations $Y^2 = X^3 + D$, where $D \in \mathbb{Z} \setminus \{0\}$ (see [7]) was extensively studied, we were unable to find in the literature an explicit solution for the case $D = 2$. In this section, we give two different solutions to the problem of finding all integral x, y satisfying the aforementioned equation. In the first one we combine factorisations in the ring of integers of $\mathbb{Q}(\sqrt{2})$ with an elementary solution to a particular cubic Thue equation. Our second solution relies on the geometric structure of the elliptic curve defined by the given affine equation.

Before going further, let us make a few remarks about the finiteness of the set of integral points on various curves. For any bivariate polynomial $f \in \mathbb{Z}[X, Y]$, let $C_f := \{(x, y) \in \overline{\mathbb{Q}}^2 : f(x, y) = 0\}$ be an affine algebraic curve. The points of C_f with coordinates in $\mathbb{Q}$ are called rational and, in general, for any $S \subseteq \overline{\mathbb{Q}}$, we denote by $C_f(S) = C_f \cap S^2$. Curves can be classified by their genus, a non-negative integer associated to their projectivization. The genus is a geometric invariant. A classical result in number theory is the following theorem

Theorem 2.1 (Siegel, 1929). *If $f \in \mathbb{Z}[X, Y]$ defines an irreducible curve C_f of genus $g(C_f) > 0$, then $C_f(\mathbb{Z})$ is finite.*

If additionally $g_f(C_f) \geq 2$, this result is superseded by the notorious Falting's theorem, which says that $C_f(\mathbb{Q})$ is also finite. Although both Siegels' and Faltings' theorems are milestones in number theory, they are "ineffective" results, meaning that their proof does not even allow one to control the size of the sets known to be finite. Therefore, they cannot be used to explicitly determine $C_f(\mathbb{Z})$ or $C_f(\mathbb{Q})$.

Effectively finding rational points on curves is an incredible difficult task and a very active topic of research. The toolbox for determining $C_f(\mathbb{Z})$ became a lot richer starting with the monumental work of Baker on linear forms in logarithms. As one of the first applications to his theory, Baker proved the following result.

Theorem 2.2 (Baker, 1969). *Suppose* $f(X,Y) = Y^2 - a_nX^n - a_{n-1}X^{n-1} - \cdots - a_0 \in \mathbb{Z}[X,Y]$, *the polynomial* $a_nX^n + \cdots + a_0$ *is irreducible in* $\mathbb{Z}[X]$, $a_n \neq 0$ *and* $n \geq 5$. *Let* $H = \max\{|a_0|, \ldots, |a_n|\}$. *Then, any integral point* $(x,y) \in C_f(\mathbb{Z})$ *satisfies*

$$\max(|x|,|y|) \leq \exp\exp\exp\{(n^{10n}H)^{n^2}\}.$$

Bounds on such solutions have been improved by many authors, but they remain astronomical and often involve inexplicit constants. Let us proceed to the resolution of our Diophantine equations.

To settle the conjecture posed by Andrica and Bagdasar in [2] and [1] which inferred that X^3+2 does not contain perfect squares when X runs through the set of positive integers, we prove the following theorem.

Theorem 2.3. *The only solutions of* $X^3 + 2 = Y^2$ *in the set of integer numbers are* $(-1,1)$ *and* $(-1,-1)$.

A few remarks are in order before giving the proof of this theorem. Since the genus of (the projectivization of) the curve determined by this equation is 1, we can use Siegel's theorem to deduce that there are finitely many points with integer coordinates. By Theorem 2.2, we know that if $(x,y) \in \mathbb{Z}^2$ is a point lying on this curve, then

$$\max(|x|,|y|) \leq \exp\exp\exp((3^{30}\cdot 2)^{3^2}).$$

Although theoretically one could now run a for loop through all possible values of x and check for which x^3+2 is a perfect square, the triple exponential bound presented above is astronomical and way out of the current computational limitations. In practice, one could check values of x up to 10^{18}, but could not hope to even get close to the aforementioned triple exponential. We proceed with the first proof of for our theorem.

3. Proof to Theorem 2.3

We will make use of the following proposition.

Proposition 3.1. *The only solution* $(a,b) \in \mathbb{Z}^2$ *to the equation*

$$a^3 + 3a^2b + 6ab^2 + 2b^3 = 1 \tag{3.1}$$

is $(a,b) = (1,0)$.

Proof. Write $f(X) = X^3 + 3X^2 + 6X + 2 \in \mathbb{Q}[X]$. It is an irreducible polynomial and let $\theta \in \overline{\mathbb{Q}}$ be any root of f. Denote by $L = \mathbb{Q}(\theta)$, the number field obtained by adjoining θ to $\mathbb{Q}$ and write $\mathcal{O}_L$ for its ring of integers. L is a degree 3 extension over $\mathbb{Q}$ and has signature $(1,1)$. We are going to denote by $\sigma_1, \sigma_2, \sigma_3 : L \hookrightarrow \mathbb{C}$ its three different complex embeddings.

It can be checked that ring of integers $\mathcal{O}_L$ is $\mathbb{Z}[\theta, \theta^2]$ and, making use of Dirichelt's unit theorem, one can compute the group of units

$$\mathcal{O}_L^\times = \langle \pm 1 \rangle \cdot \langle -\theta^2 - 3\theta - 1 \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \cdot \mathbb{Z}.$$

The element $\mu := -\theta^2 - 3\theta - 1$ is a fundamental unit, $\text{Norm}_{L/\mathbb{Q}}(\mu) = 1$ and $\text{Norm}_{L/\mathbb{Q}}(-1) = -1$. The equation (3.1) can be written as

$$\text{Norm}_{L/\mathbb{Q}}(a - b \cdot \theta) = \prod_{i=1}^{3}(a - b \cdot \sigma_i(\theta)) = 1, \text{ where } a, b \in \mathbb{Z}.$$

The above implies that $a - b\theta$ is a unit of norm 1 in O_L, hence

$$a - b\theta = \mu^n \text{ for some } n \in \mathbb{Z}. \tag{3.2}$$

We are going to use p-adic analysis to solve this last equation. We first need a local field $\mathbb{Q}_p$ into which there are three distinct embeddings of L, equivalently a prime number p such that the polynomial $X^3 + 3X^2 + 6X + 2$ has three distinct roots in $\mathbb{Q}_p$. We find $p = 79$ to be such a prime and the distinct roots are

$$\begin{array}{l} \theta_1 = 19 - 32 \cdot 79 \pmod{79^2} \\ \theta_2 = 20 - 7 \cdot 79 \pmod{79^2} \\ \theta_3 = 37 + 38 \cdot 79 \pmod{79^2} \end{array} \in \mathbb{Q}_{79}.$$

The root θ of f is mapped to r_1, r_2 and r_3 respectively, under the embeddings of L into $\mathbb{Q}_{79}$. Under the same embeddings, the fundamental unit $\mu = -\theta^2 - 3\theta - 1$ maps to

$$\begin{array}{l} \mu_1 = 55 - 37 \cdot 79 \pmod{79^2} \\ \mu_2 = 13 - 21 \cdot 79 \pmod{79^2} \\ \mu_3 = 20 - 22 \cdot 79 \pmod{79^2} \end{array} \in \mathbb{Q}_{79}.$$

By embedding the equation (3.2) into $\mathbb{Q}_{79}$, we obtain that $a - b \cdot \theta_i = \mu_i^n$ and hence $a = \mu_i^n + b \cdot \theta_i$ for $i = 1, 2$ and 3. One obtains the equality

$$(\theta_3 - \theta_2) \cdot \mu_1^n + (\theta_1 - \theta_3) \cdot \mu_2^n + (\theta_2 - \theta_1) \cdot \mu_3^n = 0$$

and since $\mu_1\mu_2\mu_3 = \text{Norm}(\mu) = 1$, we can rewrite this as

$$(\theta_3 - \theta_2) + (\theta_1 - \theta_3) \cdot (\mu_2^2\mu_3)^n + (\theta_2 - \theta_1) \cdot (\mu_2\mu_3^2)^n = 0. \tag{3.3}$$

Now $\mu_2^2\mu_3 \equiv 62 \pmod{79}$ and $\mu_2\mu_3^2 \equiv 65 \pmod{79}$. Since the left hand side of (3.3) must be equal to zero modulo 79, we can check that n is divisible by 13. Hence $n = 13 \cdot m$ for some $m \in \mathbb{Z}$.

We have that $(\mu_2^2\mu_3)^{13} \equiv 1 + 8 \cdot 79 \pmod{79^2}$ and $(\mu_2\mu_3^2)^{13} \equiv 1 + 36 \cdot 79 \pmod{79^2}$. We can now use Lemma 5.2 in [5] to expand

$$(\theta_3 - \theta_2) + (\theta_1 - \theta_3) \cdot (\mu_2^2\mu_3)^{13 \cdot m} + (\theta_2 - \theta_1) \cdot (\mu_2\mu_3^2)^{13 \cdot m} = \sum_{k=1}^{\infty} a_k \cdot m^k,$$

with $\lim\limits_{k \to \infty} \|a_k\|_{79} = 0$ and it can be checked that $\|a_1\|_{79} = 79^{-1}$ and $\|a_k\|_{79} \leq 79^{-2}$ for every $k \geq 2$. Using Strassmann's theorem (see Theorem 4.1 in [5]), we obtain that the only value of m for which $\sum\limits_{k=1}^{\infty} a_k \cdot m^k$ vanishes is $m = 0$.

This proves that $n = 0$ and replacing in (3.2) we obtain $(a, b) = (1, 0)$ is the only solution to the equation in the statement, as claimed. □

Remark 3.2. We have used the computer algebra package **Sage** [12] for basic modular arithmetic computations. The equation (3.1) is a Thue equation. It was proved that the latter have finitely many solutions and algorithms that find all of them have been implemented in various computer algebra packages. One can consult [3] for a very efficient such algorithm. The known methods for solving general Thue equations are involved, making use of Baker's bounds for linear forms in complex and of complicated reduction methods such as the one in described in loc. cit. In the above proof, we made essential use of the fact that the right

hand side of (3.1) is 1 and that the ring $\mathcal{O}_L$ has only one fundamental unit to apply p-adic analysis techniques successfully.

We now return to the proof of our theorem. Let $K = \mathbb{Q}(\sqrt{2})$ and denote by $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ its ring of integers. The later is a Dedekind domain, i.e. it is Noetherian, integrally closed in its field of fractions $\mathrm{Frac}(\mathcal{O}_K) = K$ and all its non-zero prime ideals are maximal. For any element $o \in \mathcal{O}_K$, we are going to denote by $(o) \subseteq O_K$ the principal ideal o generates.

Suppose that $x, y \in \mathbb{Z} \setminus \{0\}$ are such that $y^2 = x^3 + 2$. Therefore, in $\mathcal{O}_K$ we have the factorization $(y - \sqrt{2}) \cdot (y + \sqrt{2}) = x^3$ and the same holds for the ideals generated by these factors. It is known that ideals of $\mathcal{O}_K$ factor uniquely into prime ideals. Suppose the prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ divides both of the non-zero ideals $(y - \sqrt{2})$ and $(y + \sqrt{2})$. Then, $\mathfrak{p}$ must divide the ideal generated by the difference $y + \sqrt{2} - y + \sqrt{2} = 2\sqrt{2} = \sqrt{2^3}$. As $(\sqrt{2}) \subset \mathcal{O}_K$ is the only prime ideal of $\mathcal{O}_K$ that lies above 2, we must have $\mathfrak{p} = (\sqrt{2})$. Hence, the ideals $(y - \sqrt{2})$ and $(y + \sqrt{2})$ are coprime outside of $(\sqrt{2})$. From the previous factorization, we deduce that for every prime ideal $\mathfrak{p} \neq (\sqrt{2})$, if $\mathfrak{p}$ divides $(y - \sqrt{2})$, then $\mathfrak{p}^3$ divides the same ideal.

To see what happens in the case $\mathfrak{p} = (\sqrt{2})$, let $\mu \in \mathrm{Gal}(K/\mathbb{Q})$ be the non-trivial $\mathbb{Q}$-automorphism of K. Given a rational prime p, $\mathrm{Gal}(K/\mathbb{Q})$ acts naturally on the ideals $\mathfrak{p}$ of $\mathcal{O}_K$ that lie above p. Write $\mathfrak{p}^\mu$ for the ideal obtained from $\mathfrak{p}$ by applying μ to every element in $\mathfrak{p}$. As $\mu(\sqrt{2}) = -\sqrt{2}$, we note that $(\sqrt{2})^\mu = (-\sqrt{2}) = (\sqrt{2})$, i.e. μ stabilises the ideal above 2. Notice that $(y - \sqrt{2})^\mu = (y + \sqrt{2})$, hence the powers of $(\sqrt{2})$ that divide the ideals $(y - \sqrt{2})$ and $(y + \sqrt{2})$ are equal. Since the product $(y - \sqrt{2}) \cdot (y + \sqrt{2})$ is a third power, we conclude that the power of $(\sqrt{2})$ dividing $(y - \sqrt{2})$ must be divisible by 3.

It is an easy exercise, using for example the Minkowski bound, to prove that the class group of K is trivial. In particular, this means that every ideal of $\mathcal{O}_K$ is principal. Considering the remarks above, we have

$$(y - \sqrt{2}) = (x_0)^3 = (x_0^3), \text{ as ideals, where } x_0 \in \mathcal{O}_K.$$

We deduce that $y - \sqrt{2}$ and x_0^3 are the same up to a unit in the ring $\mathcal{O}_K$, that is there exists a unit $u \in U(\mathcal{O}_K)$ such that $y - \sqrt{2} = u \cdot x_0^3$.

By Dirichlet unit's theorem we know that $U(\mathcal{O}_K)$ is isomorphic to $T \cdot \mathbb{Z}$, where T is the finite group formed by the roots of unity that lie in K. It is an easy exercise to verify that $U(\mathcal{O}_K) = \langle -1 \rangle \cdot \langle 1 - \sqrt{2} \rangle$, so $1 - \sqrt{2}$ is the fundamental unit of $\mathcal{O}_K$. Observing that every element $u \in U(U_K)$ can be written as $u = (1 - \sqrt{2})^i \cdot (u_0)^3$ where $i \in \{-1, 0, 1\}$ and $u_0 \in U(\mathcal{O}_K) \subseteq \mathcal{O}_K$, we derive that

$$y - \sqrt{2} = (1 - \sqrt{2})^i \cdot x_1^3,$$

for some $i \in \{-1, 0, 1\}$ and $x_1 \in \mathcal{O}_K$. The element x_1 is of the form $a + b\sqrt{2}$ for $a, b \in \mathbb{Z}$. For each choice of $i \in \{-1, 0, 1\}$, by equating the coefficients of $\sqrt{2}$ in the left and right hand side of the above equation, we obtain an equality of the form

$$f(a, b) = -1 \tag{3.4}$$

where $f \in \mathbb{Z}[x, y]$ is a homogeneous cubic polynomial. When f is reducible (3.4) can be easily solved using factorization in $\mathbb{Z}$. If this is not the case and f is irreducible, the equation (3.4) is a cubic Thue equation. It is known (see for example [3]) that the latter have finitely many integral solutions and routines for determining them have been implemented in various computer algebra packages. We will appeal to Proposition 3.1 to find the solutions of the latter type of equations that arise here.

Let us analyse each of the three cases.

Case 1. $i = -1 \Rightarrow y - \sqrt{2} = (1 - \sqrt{2})^{-1} \cdot (a + b\sqrt{2})^3$.
Hence,

$$y - \sqrt{2} = -a^3 - 6a^2b - 6ab^2 - 4b^3 + \sqrt{2}\left(-a^3 - 3a^2b - 6ab^2 - 2b^3\right).$$

Using that $1, \sqrt{2}$ are linearly independent over $\mathbb{Q}$, we obtain the following two equations:

$$y = -a^3 - 6a^2b - 6ab^2 - 4b^3 \tag{3.5}$$

and

$$1 = a^3 + 3a^2b + 6ab^2 + 2b^3. \tag{3.6}$$

The variable y is an indeterminate and every solution (a, b) to (3.6) will determine a value for y. From Proposition 3.1, we know that the only solution in integers to the last equation is $a = 1$ and $b = 0$. Substituting, we see that this corresponds to $y = -1$, which implies that $x = -1$.

Case 2. $i = 0 \Rightarrow y - \sqrt{2} = (a + b\sqrt{2})^3$.

Expanding the right hand side, we see that

$$y - \sqrt{2} = a^3 + 6ab^2 + \sqrt{2}\left(3a^2b + 2b^3\right)$$

and since $1, \sqrt{2}$ are linearly independent over $\mathbb{Q}$ we must have

$$-1 = b \cdot (3a^2 + 2b^2).$$

Trying $b = \pm 1$, we see that $3a^2 + 2 = \mp 1$ is not solvable. Hence this case does not give us any solutions.

Case 3. $i = 1 \Rightarrow y - \sqrt{2} = \left(1 - \sqrt{2}\right) \cdot (a + b\sqrt{2})^3$.

This gives us

$$y - \sqrt{2} = a^3 - 6a^2b + 6ab^2 - 4b^3 + \sqrt{2}\left(-a^3 + 3a^2b - 6ab^2 + 2b^3\right),$$

which implies that

$$1 = a^3 - 3a^2b + 6ab^2 - 2b^3.$$

By making the substitution $t := -b$ in the last equation we obtain the one discussed in **Case 1**. Therefore, using Proposition 3.1 once again we find $a = 1$, $b = 0$ and hence $y = 1$. Using that $y^2 = x^3 + 2$, we get that $x = -1$. The proof of our theorem is now complete.

In the proof above we made explicit use of the fact that $\mathbb{Q}(\sqrt{2})$ has trivial class group, information that allowed us to pass from factorisations of ideals to nice factorisations of elements in the ring $\mathbb{Z}[\sqrt{2}]$. In general, for $D \in \mathbb{Z}$ the ideal class group of $\mathbb{Q}(\sqrt{D})$ can be arbitrary large so our first strategy will not work for more general Mordell equations. The second proof of our theorem can be adapted to find all the integral solutions of $Y^2 = X^3 + D$ for any fixed $D \in \mathbb{Z}$.

The given problem is one of explicitly determining the integral points on the affine curve given by $Y^2 = X^3 + 2$. These can be found by exploiting its rich geometric structure, as presented below.

4. Alternate proof to Theorem 2.3

The geometry of the curve is better captured by its projectivization

$$E := Y^2Z = X^3 + 2Z^3 \in \mathbb{P}^2(\mathbb{C}), \tag{4.1}$$

a non-singular projective curve of genus 1, which contains the point $\mathcal{O} = [0 : 1 : 0] \in \mathbb{P}^2(\mathbb{Q})$, commonly called "the point at infinity". The point at infinity is the only one on the projective curve that does not naturally project on our chosen affine model. The set of complex points on E can be given an abelian group structure for which the distinguished point $\mathcal{O}$ acts as the identity element. The group law is given by chord-tangent formulas and therefore it is easy to see that $E(\mathbb{Q})$ is a subgroup of $E(\mathbb{C})$. By a famous theorem of Mordell, we know that $E(\mathbb{Q}) \cong T \times \mathbb{Z}^r$ (as abstract abelian groups) where T is a finite group, commonly called *the torsion subgroup* and r is a positive integer called the *rank*.

Using the Lutz-Nagell theorem (see Corollary 7.2 in [11]), it is easy to deduce that T is included in $\{\mathcal{O}, P, -P\}$, where $P = [-1 : 1 : 1]$ and $-P = [-1 : -1 : 1]$ are inverses of each other under the group law. Using the formulae for addition on the elliptic curve, we compute all the values of $2 \cdot P, \ldots, 12 \cdot P$ and observe that none of them is equal to the origin $\mathcal{O}$. For example, $5 \cdot P = [108305279/48846121 : 1226178094681/341385539669 : 1] \neq \mathcal{O}$, and the larger multiples of P involve denominators that are too big to fit in one line. In his seminal article [9], Mazur gave a classification of all the possible isomorphisms types for the torsion group of an elliptic curve defined over $\mathbb{Q}$. From there, we see that the order of any torsion point is at most 12 and therefore we can conclude that P has infinite order.

The non-torsion part of $E(\mathbb{Q})$ is in general extremely difficult to compute. Even computing the rank of a given elliptic curve is, in general, a notorious problem. The latter quantity features in the famous Birch and Swinnerton-Dyer conjecture, one of the Millenium Problems. There are implementations of algorithms that succeed most of the times in computing the rank and finding generators. By running one such, namely John Cremona's **mwrank** algorithm implemented in **Sage** [12], we prove unconditionally that $r = 1$ and P is the generator of $E(\mathbb{Q})$. Just to sum up,

$$E(\mathbb{Q}) = \langle P \rangle \cong \mathbb{Z},$$

so all the points with rational coordinates on the projective curve are of the form $k \cdot P$, for $k \in \mathbb{Z}$. By computing with the group law, one can observe that $2 \cdot P = [17/4 : -71/8 : 1]$ and $-2 \cdot P = [17/4 : 71/8 : 1]$. As $|k| \geq 2$, the experiments suggest that the coordinates of $k \cdot P$ have denominators that grow extremely fast. We should remark that we always set the last coordinate $Z = 1$, as we are interested in the image of these points on the affine curve.

Suspecting that P and $-P$ are the only points with integral affine coordinates, we will use the program **integral_points** implemented in **Sage** by Cremona to prove it. The algorithm behind **integral_points** is described in Section 8.7 of [6]. We will mention briefly that this algorithm relies on a deep generalisation of Baker's theorem due to David and Hirata-Köhno [8], which if applied to our setup proves that if $|k| > e^{100}$ then $k \cdot P$ does not have integral coordinates on our affine model. Additionally, the aforementioned algorithm includes a clever application of the **LLL** reduction algorithm to reduce the bound e^{100} to 13, in our case. After this reduction, the program tests which of $k \cdot P$ are integral, when $k \leq 13$. The **Sage** program **integral_points** requires as input our elliptic curve E and a list of generators for the Mordell-Weil group $E(\mathbb{Q})$. It returns as output all the points in $E(\mathbb{Z})$. We refer the reader to Section 8.7 of [6] for a deeper understanding of **integral_points** and of the **Sage** output below, which proves our theorem.

```
sage: E = EllipticCurve([0,2]);
sage: E
Elliptic Curve defined by y^2 = x^3 + 2 over Rational Field
sage: P = E(-1,1)
sage: E.integral_points(mw_base = [P], both_signs = True, verbose = True)
Using mw_basis  [(-1 : 1 : 1)]
e1,e2,e3:  0.629960524947437 - 1.09112363597172*I,
 0.629960524947437 + 1.09112363597172*I, -1.25992104989487
Minimal and maximal eigenvalues of height pairing matrix:
 0.754576903181227,0.754576903181227
x-coords of points on non-compact component with  -1 <=x<= 2
[-1]
starting search of remaining points using coefficient bound 4 and
 |x| bound 184648.204428771
x-coords of extra integral points:
[-1]
```

```
Total number of integral points: 2
[(-1 : -1 : 1), (-1 : 1 : 1)]
```

Acknowledgements. The authors are very grateful to the anonymous referee for suggesting several significant improvements and simplifications to earlier versions of this paper.

References

[1] Andrica, D., Bagdasar, O., *The Cauchy integral formula with applications to polynomials, partitions and sequences*, Proceedings of the XV$^{\text{th}}$ Int. Conf. on Mathematics and its Applications, Timişoara, Romania, November 1-3, 2018 Romania, Editura Politehnica, Timişoara, 2019, 12-25.

[2] Andrica, D., Bagdasar, O., *On k-partitions of multisets with equal sums*, submitted.

[3] Bilu, Y., Hanrot, G., *Solving Thue equations of high degree*, Journal of Number Theory, **60**(1996), no. 2, 373-392.

[4] Bosma, W., *The Magma algebra system 1. The user language*, **24**(1997).

[5] Cassels, J. , *Local Fields*, Cambridge University Press, 1986.

[6] Cohen, H., *Number Theory Volume I: Tools and Diophantine Equations*, Springer, 2007.

[7] Conrad, K., *Examples of Mordell's equation*, survey article available online at https://kconrad.math.uconn.edu/blurbs/gradnumthy/mordelleqn1.pdf.

[8] David, S., Hirata-Köhno, N., *Linear forms in logarithms*, J. Reine Angew. Math., **628**(2009), 37-89.

[9] Mazur, B., *Rational isogenies of prime degree*, Invent. Math., **44**(1978), no. 2, 129-162.

[10] OEIS, *The online encyclopedia of integer sequences*, published electronically at http://oeis.org, 2018.

[11] Silverman, J. H., *The Arithmetic of Elliptic Curves*, Springer GMT, **106**(1986).

[12] The Sage Developers, *Sagemath, the Sage Mathematics Software system*, Version 8.5, 2018.

[13] Waldschmidt, M., *Perfect powers: Pillai's works and their developments*, arxiv:0908.4031v1[math.NT], 27 Aug 2009.

Dorin Andrica
Babeş-Bolyai University
Faculty of Mathematics and Computer Sciences
1, Kogălniceanu Street
400084 Cluj-Napoca, Romania
e-mail: dandrica@math.ubbcluj.ro

George C. Ţurcaş
University of Warwick
Mathematics Institute
CV4 7AL, Coventry, United Kingdom
e-mail: g.c.turcas@warwick.ac.uk