Acta Universitatis Apulensis
ISSN: 1582-5329
http://www.uab.ro/auajournal/

No. 58/2019
pp. 83-90
doi: 10.17114/j.aua.2019.58.07

THE NUMBER OF INTEGRAL SOLUTIONS TO AN EQUATION INVOLVING SUMS OF RADICALS

Dorin Andrica and George Cătălin Ţurcaş

Abstract. In this short note, we present a Galois-theoretic proof for the following result. Given an integer $k \geq 2$ and fixed positive integers $n_1, \ldots, n_k$, the number of solutions $(x_1, \ldots, x_k, y) \in (\mathbb{Z}_{\geq 0})^{k+1}$ to the equation (1) is finite. This generalises a problem proposed by the authors and selected for the final round of the Romanian Mathematical Olympiad in 2019. In Theorem 2, we prove an interesting lower bound for the number of such solutions in the particular case when $n_1 = \cdots = n_k = n$. This lower bound involves the number of divisors function. In the same case, we formulate two conjectures regarding the sequence generated by the number of such solutions. In the first conjecture, we speculate that when $k = 2$, the sequence takes every positive integer value. The second conjecture concerns an asymptotic of that should hold for general values of $k \geq 2$. These are supported by extensive computer calculations.

2010 *Mathematics Subject Classification*: 11B99, 11A25.

Keywords: radicals, number of divisors, Galois theory.

1. Introduction

The authors proposed the following number theory problem to the final round of the 70-th National Mathematical Olympiad.

Problem (ONM 2019)**.** For every positive integer n, we define the set

$$A_n = \left\{ (x, y) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \;\middle|\; \sqrt{x^2 + y + n} + \sqrt{y^2 + x + n} \in \mathbb{Z}_{\geq 0} \right\}.$$

Show that for every $n \geq 1$, the set A_n is non-empty and finite.

This left a very good impression on the problem selection committee, which selected it for the competition. Although it admits an elementary solution, the

problem asks to prove that there are finitely many integral points on the degree 4 algebraic surface

$$(x^2+y+n)^2+(y^2+x+n)^2+z^4 = 2(x^2+y+n)(y^2+x+n)+2(x^2+y+n)z^2+2(y^2+x+n)z^2.$$

In fact, this a a family, depending on n, of Diophantine equations in variables x, y, z. The study of such problems can be notoriously difficult and represents a central topic of research for modern number theorists (see [1] and [4]).

Figure 1 constitutes of a plot for the connected component corresponding to $z \geq 0$ of the algebraic surface described above, in the particular case $n = 10$. The plot was produced using Mathematica [6] and all points with non-negative integral coordinates lying on the surface are marked with red dots. The latter are $\{(1, 5, 10), (2, 2, 8), (3, 6, 12), (5, 1, 10), (6, 3, 12), (9, 9, 20)\}$.

The purpose of this short note is twofold. Firstly, we present a Galois-theoretic approach to a generalisation of the problem above. Secondly, we show that there is a lower bound on the number of pairs in A_n that depends on the number of divisors of $4n - 1$.

We will prove the following two theorems.

Theorem 1. *Given an integer $k \geq 2$ and $n_1, \ldots, n_k \in \mathbb{Z}_{>0}$, the number of solutions in $(x_1, \ldots, x_k, y) \in (\mathbb{Z}_{\geq 0})^{k+1}$ to the equation*

$$\sum_{i=1}^{k} \sqrt{x_i^2 + x_{i+1} + n_i} = y, \tag{1}$$

where $x_{k+1} = x_1$, is finite.

Our result is strongly related to the problem of linear independence (over $\mathbb{Q}$) of radicals. This is proved in [2] (see pages 419-420) using the fundamental theorem of symmetric polynomials. A beautiful survey of the problem can be found in [3].

For the particular case when $n_1 = \cdots = n_k = n$, let us denote by $A_n^{(k)}$ the set of solutions $(x_1, \ldots, x_k, y) \in (\mathbb{Z})^{k+1}$ to the equation (1). It is interesting to estimate the size of the finite set $A_n^{(k)}$. We prove the following lower bound, which shows that $\limsup_{n\to\infty} \left|A_n^{(k)}\right| = +\infty$.

Theorem 2. *For every n, k as above, we have*

$$\left|A_n^{(k)}\right| \geq \frac{\tau\left(4n-1\right)}{2},$$

where $\tau : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ is the number of divisors function.

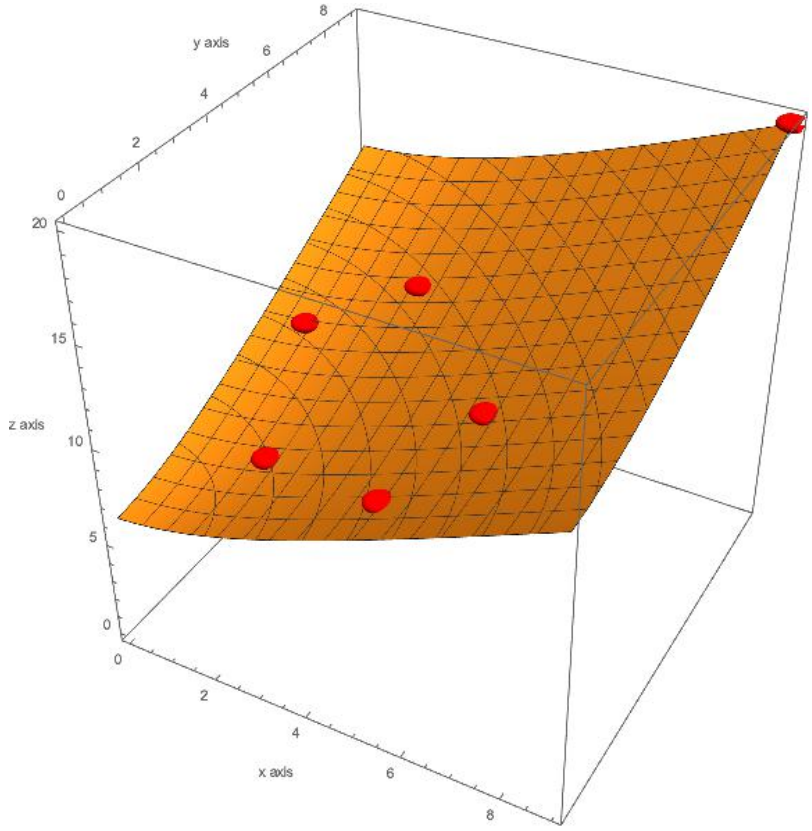

Figure 1: Connected component with $z \geq 0$ of the algebraic surface for $n = 10$.

2. Proof of Theorem 1

We first give an elementary proof of finiteness in the case $k = 2$. Suppose that $(x_1, x_2, y) \in (\mathbb{Z}_{\geq 0})^3$ is a solution to (1). Squaring, one notices that the product

$$2 \cdot \sqrt{(x_1^2 + x_2 + n_1)(x_2^2 + x_1 + n_2)} \in \mathbb{Z}_{>0}$$

and hence

$$\sqrt{x_1^2 + x_2 + n_1} - \sqrt{x_2^2 + x_1 + n_2} = \frac{x_1^2 - x_2^2 + x_2 - x_1}{\sqrt{(x_1^2 + x_2 + n_1)(x_2^2 + x_1 + n_2)}} \in \mathbb{Q}.$$

One obtains that $\sqrt{x_1^2 + x_2 + n_1}$ and $\sqrt{x_2^2 + x_1 + n_2}$ are both rational numbers, hence integers.

Now $x_1^2+x_2+n_1 > x_1^2$, so we must have that $x_1^2+x_2+n_1 \geq (x_1+1)^2$. Similarly, $x_2^2+x_1+n_2 \geq (x_2+1)^2$. Summing up the last two inequalities, we obtain that $n_1+n_2-2 \geq x_1+x_2$ thus there are finitely many possibilities for choosing x_1, x_2. Each such choice determines y, therefore the equation (1) has finitely many solutions.

Additionally, it is possible to give such elementary proofs for the finiteness of the number of solutions to (1) when $k \in \{3,4\}$. Unfortunately, this approach does not extend for $k \geq 5$.

Although this problem seems to be elementary, it generates complicated other problems in number theory. To emphasize one such, we stay in the case $k=2$ and we consider $n_1 = n_2 = n$. Define the sequence $(a_n)_{\geq 1}$, such that $a_n = |A_n^{(2)}|$ for every $n \geq 1$. The first few values of $(a_n)_{\geq 1}$ are

1, 1, 3, 2, 1, 1, 2, 3, 2, 6, 3, 1, 2, 2, 3, 5, 5, 1, 3, 1, 5, 2, 2, 6, 3, 5, 1, 2, 2, 2, 8, 5, 3, 4, 3, 6, 3, 3, 4, 4, 3, 3, 7, 3, 3, 4, 2, 5, 4, 1, 8, 9, 1, 6, 6, ...

This sequence is not yet indexed in The On-Line Encyclopedia of Integer Sequences (OEIS). We have that $a_{1536} = 29$ and every positive integer less than or equal to 29 appears as some term in $(a_n)_{\geq 1}$. Computer assisted calculations suggest the following interesting phenomena.

Conjecture 1. Every positive integer appears as one of the terms of the sequence $(a_n)_{\geq 1}$.

We give a general proof that the number of solutions to (1) is finite. All the Galois theory concepts we use can be found in any classical Galois theory textbook (see, for instance Cox [5]).

Let $(x_1, \ldots, x_k, y) \in (\mathbb{Z}_{\geq 0})^{k+1}$ be a solution to (1). We therefore have

$$\sum_{i=1}^{k} \sqrt{x_i^2 + x_{i+1} + n_i} \in \mathbb{Z}_{>0}, \tag{2}$$

where $x_{k+1} = x_1$. We claim that each summand in (2) is an integer. Proceeding by contradiction, assume this is not the case.

Let $S \subseteq \{1, \ldots, k\}$ be defined by the following algorithm.

- Start with $S := \{1, \ldots, k\}$.
- For each $i \in S$, if $\sqrt{x_i^2 + x_{i+1} + n_i} \in \mathbb{Z}$ then $S := S \setminus \{i\}$.
- For every pair $(i,j) \in S^2$ such that $i < j$, if $\frac{\sqrt{x_j^2+x_{j+1}+n_j}}{\sqrt{x_i^2+x_{i+1}+n_i}} \in \mathbb{Q}$, then $S := S \setminus \{j\}$.

Our assumption implies that $|S| \geq 2$ at the end of this sequence of steps.

We can now see that there are positive rational numbers c_i such that

$$\sum_{i \in S} c_i \cdot \sqrt{x_i^2 + x_{i+1} + n_i} \in \mathbb{Q} \tag{3}$$

and each two of the square roots in the sum (3) are linearly independent over $\mathbb{Q}$. The desired conclusion follows if we prove that all the square roots in the sum above are rationals, hence integers.

Let K_S be the (finite) extension of $\mathbb{Q}$ formed by adjoining $\sqrt{x_i^2 + x_{i+1} + n_i}$ for all $i \in S$. It is the smallest field that contains $\mathbb{Q}$ and all the square roots appearing in (3).

Let T be a subset of S, of minimal cardinality, such that

$$K_S = \mathbb{Q}\left(\left\{\sqrt{x_i^2 + x_{i+1} + n_i} : i \in T\right\}\right).$$

Our construction of $|S|$ implies that $|T| \geq 2$ as well. An important feature of the square-roots appearing in $\left\{\sqrt{x_i^2 + x_{i+1} + n_i} : i \in T\right\}$ is that they are multiplicatively independent, namely no product of any subset of them is rational.

The field extension $K_S/\mathbb{Q}$ is Galois of order $2^{|T|}$. Its Galois group $\mathrm{Gal}(K_S/\mathbb{Q})$ consists of all field automorphisms $\sigma : K_S \to K_S$ that fix $\mathbb{Q}$. Every such automorphism $\sigma \in \mathrm{Gal}(K_S/\mathbb{Q})$ is completely determined by its image on the generators of K_S over $\mathbb{Q}$, i.e. on the set

$$\left\{\sqrt{x_i^2 + x_{i+1} + n_i} : i \in T\right\}.$$

For every $i \in S$, and every $\sigma \in \mathrm{Gal}(K_S/\mathbb{Q})$ we have that

$$\sigma^2\left(\sqrt{x_i^2 + x_{i+1} + n_i}\right) = \sigma(x_i^2 + x_{i+1} + n) = x_i^2 + x_{i+1} + n_i,$$

so $\sigma\left(\sqrt{x_i^2 + x_{i+1} + n_i}\right) = \pm\sqrt{x_i^2 + x_{i+1} + n_i}$ and each such choice for the elements $i \in T \subseteq S$, gives a different automorphism of $\mathrm{Gal}(K_S/\mathbb{Q})$.

We will prove that (3) implies that $\sqrt{x_i^2 + x_{i+1} + n_i} \in \mathbb{Z}$ for every $i \in S$, yielding our desired contradiction, by induction on $|S|$.

The conclusion follows trivially if $|S| = 2$.

When $|S| > 2$, we fix an $i_0 \in T \subseteq S$. An easy consequence of Galois theory for the extension $K_S/\mathbb{Q}$ implies that there exists $\sigma_i \in \mathrm{Gal}(K_S/\mathbb{Q})$, a $\mathbb{Q}$-automorphism

of K_S, such that $\sigma_{i_0}\left(\sqrt{x_{i_0}^2+x_{i_0+1}+n_{i_0}}\right) = -\sqrt{x_{i_0}^2+x_{i_0+1}+n_{i_0}}$ and for every $i \in T \setminus \{i_0\}$, we have that $\sigma_{i_0}\left(\sqrt{x_i^2+x_{i+1}+n_i}\right) = \sqrt{x_i^2+x_{i+1}+n_i}$.

By definition, σ_{i_0} fixes the sum (3), since the latter is a rational number. Each summand in the sum (3) is either fixed or sent to its negative by σ_{i_0}. It is essential that at least one summand in the sum is fixed, a consequence of the fact that $|T| \geq 2$. Applying σ_{i_0} to (3), we obtain

$$\sum_{i \in S'} c_i \cdot \sqrt{x_i^2+x_{i+1}+n_i} \in \mathbb{Q}, \text{ where } S' \subsetneq S.$$

The conclusion follows from the induction hypothesis.

We therefore proved that $x_i^2+x_{i+1}+n_i$ are perfect squares for every $i \in \{1,\ldots,k\}$. For each such index i, the inequality $x_i^2+x_{i+1}+n_i > x_i^2$ implies that

$$x_i^2+x_{i+1}+n_i \geq (x_i+1)^2.$$

Summing up the above inequality for all $i \in \{1,\ldots,k\}$, we get

$$\sum_{i=1}^{k} x_i^2+x_{i+1}+n_i \geq \sum_{i=1}^{k}(x_i+1)^2,$$

which is equivalent to

$$\sum_{i=1}^{k}(n_i-1) \geq \sum_{i=1}^{k} x_i.$$

As the numbers x_i are non-negative integers, the last inequality implies that the number of solutions in $(x_1,\ldots,x_k) \in (\mathbb{Z}_{\geq 0})^k$ to the equation (1) is finite. This proof gives the näive upper bound $\sum\limits_{r=0}^{B}\binom{r+k-1}{k-1}$, where $B = \sum\limits_{i=1}^{k}(n_i-1)$, for the number of such solutions.

Corollary 3. *Given an integer $k \geq 2$ and $n_1,\ldots,n_k \in \mathbb{Z}_{>0}$, there exists a minimal constant $\rho(n_1,\ldots,n_k) > 0$ such that for every $m = (m_1,\ldots,m_k) \in \mathbb{Z}^k$ with $||m|| > \rho(n_1,\ldots,n_k)$, the system of equations*

$$\begin{cases} x_1^2+x_2+n_1 = m_1^2 \\ x_2^2+x_3^2+n_2 = m_2^2 \\ \cdots\cdots\cdots\cdots\cdots \\ x_k^2+x_1^2+n_k = m_k^2 \end{cases} \tag{4}$$

has no solutions in the unknowns $x_1,\ldots,x_k$.

We remark that a simple computation shows that

$$\rho(n_1,\ldots,n_k) < \left(\sum_{i=1}^{k}(n_i-1)\right)^2 + 2\sum_{i=1}^{k} n_i - k.$$

Finding a sharp upper bound for $\rho(n_1,\ldots,n_k)$ seems to be a difficult, but interesting problem.

3. Proof of Theorem 2

In the present section we derive an interesting lower bound for the number of solutions to the equation (1), in the particular case in which $n = n_1 = \ldots = n_k$.

We claim that the number of k-tuples $(x,\ldots,x) \in A_n^{(k)}$ is equal to the announced lower bound.

Let m be a positive integer such that $x^2 + x + n = m^2$. We have that

$$4m^2 = (2x+1)^2 + 4n - 1$$

and therefore

$$(2m - 2x - 1)\cdot(2m + 2x + 1) = 4n - 1.$$

In the equation above, given n we must find values for $x \in \mathbb{Z}_{\geq 0}$ and $m \in \mathbb{Z}_{>0}$.

We observe that

$$2m - 2x - 1 = d \text{ and } 2m + 2x + 1 = \frac{4n-1}{d}, \tag{5}$$

where $d \leq \sqrt{4n-1}$ is a divisor of $4n-1$. The system of equations (5) can be rewritten as

$$4m = d + \frac{4n-1}{d} \text{ and } 4x = \frac{4n-1}{d} - d - 2. \tag{6}$$

We can solve the system of equations (6) and find values for m and x if and only if $\{d \pmod 4, (4n-1)/d \pmod 4\} = \{1 \pmod 4, 3 \pmod 4\}$. This holds, since $4n-1 = 3 \pmod 4$ and its divisors come in pairs $(d, \frac{4n-1}{d})$ satisfying the above. For each such divisor pair, the system (6) has a unique solution (m,x). The number of such pairs is $\tau(4n-1)/2$, hence our theorem is proved.

Remark 1. *For $n = 2019$ and $k = 2$, we have $\left|A_n^{(k)}\right| = 18$. The number of divisors of $4\cdot 2019 - 1$ is 12 and they determine the 6 pairs $(2,2)$, $(74,74)$, $(101,101)$, $(114,114)$, $(402,402)$ and $(2018,2018)$. With the aid of a computer, we also found that $(1,96)$, $(12,337)$, $(24,109)$, $(29,56)$, $(88,1053)$, $(864,1441)$ and their reciprocals belong to $A_{2019}^{(2)}$.*

Extensive computer computations suggest the following conjecture regarding an asymptotic formula for the size of $A_n^{(k)}$.

Conjecture 2. For fixed $k \geq 2$, we have that

$$\left|A_n^{(k)}\right| = \frac{\tau(4n-1)}{2} + o(n),$$

where $o(n)$ is the usual small-o notation, which essentially means that

$$\lim_{n\to\infty} \frac{1}{n}\left(\left|A_n^{(k)}\right| - \frac{\tau(4n-1)}{2}\right) = 0.$$

It is very hard to test this conjecture for large values of k, since the complexity of computer algorithms for determining $A_n^{(k)}$ grow exponentially in k.

References

[1] T. Andreescu, D. Andrica, I. Cucurezeanu, *An Introduction to Diophantine Equations*, Birkhäuser, Boston, 2010.

[2] T. Andreescu, G. Dospinescu, *Straight from the Book*, XYZ Press, 2012.

[3] I. Boreico, *My Favorite Problem: Linear Independence of Radicals*, Harvard College Math. Rev. 2, 1 (2008), 87-92.

[4] P. Corvaja, U. Zannier, *On integral points on surfaces*, Ann. of Math. 2, 160 (2004), 705-726.

[5] D. A. Cox, *Galois theory*, John Wiley & Sons, 2012.

[6] Wolfram Research, Inc., *Mathematica*, Version 12.0, Champaign, IL (2019).

Dorin Andrica
Faculty of Mathematics and Computer Sciences
"Babeş-Bolyai" University,
Cluj-Napoca, Romania
email: *dandrica@math.ubbcluj.ro*

George C. Ţurcaş
Mathematics Institute,
University of Warwick,
Coventry, United Kingdom
email: *George.Turcas@warwick.ac.uk*