Arch. Math. 115 (2020), 279–287
© 2020 The Author(s).
0003-889X/20/030279-9
published online 29 May 2020
https://doi.org/10.1007/s00013-020-01480-1

Archiv der Mathematik

Sums of S-units in the solution sets of generalized Pell equations

L. Hajdu and P. Sebestyén

Abstract. In this paper, we give various finiteness results concerning solutions of generalized Pell equations representable as sums of S-units with a fixed number of terms. In case of one term, our result is effective, while in case of more terms, we are able to bound the number of solutions.

Mathematics Subject Classification. 11D09, 11D61, 11B37.

Keywords. Generalized Pell equation, Recurrence sequences, Sums of S-units, S-unit equations.

1. Introduction. There are many papers about equations of the form

$$U_n = z_1 + \cdots + z_k, \tag{1}$$

where $(U_n)_{n=0}^{\infty}$ is a linear recurrence sequence, and $z_1, \ldots, z_k$ are integers with prime factors coming from a fixed finite set of primes. Here we only refer to the recent papers Guzman-Sanchez and Luca [8], Bertók et al. [1], Bérczes et al. [2], and the (many) references there, where several and various finiteness results have been proved. We mention that there are also many results in the literature where other related problems are discussed. For example, Bravo et al. [4] considered a problem connected to sums of terms of a recurrence sequence yielding perfect powers (also see the references there).

In this paper, we consider the problem of representability of solutions of generalized Pell equations as a fixed term sum of integers with prime factors coming from some finite set of primes. As we shall see, this problem is closely related to Eq. (1). In fact, the problem is more general: it turns out that we need to find sums of the form $z_1 + \cdots + z_k$ in unions of recurrence sequences, rather than in only one fixed sequence. We note that there are some closely related results in the literature. We mention only two recent papers Luca and

Research supported in part by the NKFIH Grants 115479, 128088, and 130909, and the Projects EFOP-3.6.1-16-2016-00022 and EFOP-3.6.2-16-2017-00015 co-financed by the European Union and the European Social Fund.

Birkhäuser

Togbé [11] and Ddamulira and Luca [5] about the x-coordinates of certain Pell-equations which are (generalized) Fibonacci numbers, and the references therein, and a very fresh one by Erazo et al. [6] on linear combinations of prime powers in the x-coordinates of solutions of Pell equations.

2. New results. Before formulating our theorem, we need to introduce some new notation.

The equation

$$x^2 - dy^2 = t \tag{2}$$

is called a generalized Pell equation, where $d, t \in \mathbb{Z}$, $d > 1$ is square-free, and t is a non-zero integer. (Note that the name Pell equation usually refers to the cases $t = \pm 1, \pm 4$, while for the other values of t, (2) is a norm form equation in $\mathbb{Q}(\sqrt{d})$.) Write X and Y for the sets of solutions of Eq. (2) in $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$, respectively.

Let $p_1, \dots, p_\ell$ be distinct primes and put $S = \{p_1, \dots, p_\ell\}$. Then a rational number z is an S-unit if z can be written as

$$z = \pm p_1^{b_1} \cdots p_\ell^{b_\ell}$$

with some $b_1, \dots, b_\ell \in \mathbb{Z}$. Write U_S for the set of S-units.

Further, for $\gamma \in \mathbb{Q}$, write $h(\gamma)$ for the maximum of the absolute values of the numerator and the denominator of γ. Finally, for a non-zero integer m, let $\omega(m)$ denote the number of distinct prime divisors of $|m|$.

Now we can give our results about sums of S-units in the solution sets of generalized Pell equations. In the particular case of 'one-term' sums, our theorem is effective, that is, we are able to bound all the parameters involved. In the general case, we can bound only the number of solutions.

Theorem 2.1. *Use the above notation, and let $k \geq 1$. Then there are at most c_1 tuples $(z_1, \dots, z_k) \in U_S^k$ such that*

$$z_{i_1} + \cdots + z_{i_j} \neq 0 \tag{3}$$

for any $0 < j \leq k$ and $1 \leq i_1 < \cdots < i_j \leq k$, and

$$z_1 + \cdots + z_k \in X \cup Y, \tag{4}$$

where c_1 is an effectively computable constant depending only on $\omega(t)$, k, and ℓ. Further, if $k = 1$, then we also have

$$h(z_1) < c_2,$$

where c_2 is an effectively computable constant depending only on d, t, and S.

Remark. Schinzel [13] proved that the greatest prime divisor of $f(x)$, where f is a quadratic polynomial with integer coefficients having distinct roots, effectively tends to infinity as $|x| \to \infty$. From this, the case $k = 1$ of the above theorem easily follows. However, to keep the presentation coherent, we shall give a general proof of Theorem 2.1, ultimately based upon the theory of S-unit equations.

We also note that the condition (3) is not only natural, but it is necessary, as well. Indeed, if for some $z_1, \dots, z_k$, we have (4), but (3) does not hold for some $0 < j \le k$ and $1 \le i_1 < \dots < i_j \le k$, then the sums

$$z_1 + \dots + z_k + (z_0 - 1)(z_{i_1} + \dots + z_{i_j}) \quad (z_0 \in U_S)$$

would yield infinitely many solutions for the inclusion (4).

3. The proof of Theorem 2.1. To prove our theorem, we need several lemmas. The first one describes the solutions of Eq. (2) in the particular, but very important case $t = 1$.

Lemma 3.1. *Let u_0 and v_0 be the smallest positive solutions (in x and y, respectively) of the equation*

$$x^2 - dy^2 = 1. \tag{5}$$

Then all positive integer solutions u, v of (5) are given by

$$u + \sqrt{d}v = \left(u_0 + \sqrt{d}v_0\right)^m \quad (m \ge 1).$$

Proof. The statement is [12, Theorem 7.26, p. 354]. □

Before formulating our further lemmas, we need to introduce some notation concerning recurrence sequences. Let A, B be integers with $B \ne 0$, and let U_0, U_1 be integers such that at least one of them is non-zero. Then the sequence $U = (U_n)_{n \ge 0}$ satisfying the relation

$$U_n = AU_{n-1} + BU_{n-2} \quad (n \ge 2) \tag{6}$$

is called a binary linear recurrence sequence. We shall also use the notation $U = U(A, B, U_0, U_1)$ for the sequence. The characteristic polynomial of U is defined by

$$f(x) := x^2 - Ax - B.$$

Write α and β for the roots of $f(x)$. The sequence U is called degenerate if α/β is a root of unity; otherwise it is called non-degenerate. It is well-known that if U is non-degenerate, then we have

$$U_n = \frac{(U_1 - U_0\beta)\alpha^n - (U_1 - U_0\alpha)\beta^n}{\alpha - \beta} \quad (n \ge 0). \tag{7}$$

Our second lemma shows that the sets of the coordinates of the solutions of Eq. (2) are unions of finitely many non-degenerate binary linear recurrence sequences. We note that this assertion is long and well-known qualitatively. However, we do not know any source where this statement is explicitly formulated (let alone the paper of Liptai [10] which is in Hungarian). In fact, we shall only need the case concerning solutions with $\gcd(x, y) = 1$. However, we find the general case of possible independent interest. For a non-negative integer m, write $\tau(m)$ for the number of divisors of $|m|$.

Lemma 3.2. *Let u_0 be as in Lemma 3.1. If Eq. (2) has a solution, then all its solutions are given by*

$$(x,y) = \left(G_n^{(i)}, H_n^{(i)}\right) \quad (i = 1,\dots,I)$$

with some binary recurrence sequences

$$G^{(i)} = G^{(i)}(2u_0, -1, G_0^{(i)}, G_1^{(i)}), \quad H^{(i)} = H^{(i)}(2u_0, -1, H_0^{(i)}, H_1^{(i)}).$$

Here I and $G_0^{(i)}, G_1^{(i)}, H_0^{(i)}, H_1^{(i)}$ $(i = 1,\dots,I)$ are some positive integers with $I < c_3$ and

$$|G_j^{(i)}|, |H_j^{(i)}| < c_4 \ (0 \le j \le 1,\ 1 \le i \le I), \tag{8}$$

where c_3 is an effectively computable constant depending only on $\tau(t)$, while c_4 is an effectively computable constant depending only on d and t. Further, for the solutions (x,y) of (2) with $\gcd(x,y) = 1$, the same conclusion holds with $I < c_5$ and (8), where c_5 is an effectively computable constant depending only on $\omega(t)$.

Proof. Obviously, we may restrict to positive integer solutions of (2). So let (p,q) be a positive solution of (2). Then the norm $N(p+\sqrt{d}q)$ of the algebraic integer $p+\sqrt{d}q$ is t in the field $\mathbb{Q}(\sqrt{d})$. By [9, Lemma 5], we know that there are only finitely many pairwise non-associate algebraic integers $U + V\sqrt{d}$ in $\mathbb{Q}(\sqrt{d})$ of norm t, and their number I can be bounded in terms of $\tau(t)$; further, under the assumption $\gcd(p,q) = 1$, even in terms of $\omega(t)$. It is well-known (see, e.g., [14, Chapter A]) that we may assume here that

$$\max(|U|, |V|) < c_6,$$

where c_6 is an effectively computable constant depending only on d, t. Thus there exist algebraic integers $U_i + \sqrt{d}V_i$ with $N(U_i + \sqrt{d}V_i) = t$ and $\max(|U_i|, |V_i|) < c_6$ $(i = 1,\dots,I)$ such that

$$p + \sqrt{d}q = \nu(U_i + \sqrt{d}V_i)$$

for some $1 \le i \le I$, where ν is a unit in $\mathbb{Q}(\sqrt{d})$. We immediately get that $N(\nu) = 1$. Thus Lemma 3.1 yields that

$$\nu = \pm(u_0 + \sqrt{d}v_0)^z \ \ (z \in \mathbb{Z}).$$

For simplicity, we assume that $\nu = (u_0 + \sqrt{d}v_0)^m$ with some $m \ge 0$ since all the other cases are similar (or can be excluded by our assumption that p and q are positive). Then we have

$$p + \sqrt{d}q = (U_i + \sqrt{d}V_i)(u_0 + \sqrt{d}v_0)^m,$$

whence also

$$p - \sqrt{d}q = (U_i - \sqrt{d}V_i)(u_0 - \sqrt{d}v_0)^m.$$

Putting

$$\alpha := u_0 + \sqrt{d}v_0, \quad \beta := u_0 - \sqrt{d}v_0,$$

from these assertions, we obtain

$$p = \frac{U_i + \sqrt{d}V_i}{2}\alpha^m + \frac{U_i - \sqrt{d}V_i}{2}\beta^m$$

and

$$q = \frac{U_i + \sqrt{d}V_i}{2\sqrt{d}}\alpha^m - \frac{U_i - \sqrt{d}V_i}{2\sqrt{d}}\beta^m.$$

Hence, as α, β are roots of the polynomial $x^2 - 2u_0x + 1$ (also in view of (7)), we get that p and q are elements of the recurrence sequences $G = G(A, B, G_0^{(i)}, G_1^{(i)})$ and $H = H(A, B, H_0^{(i)}, H_1^{(i)})$, respectively, with

$$A = 2u_0, \quad B = -1,$$

and

$$(G_0^{(i)}, G_1^{(i)}) = (U_i, u_0U_i + dv_0V_i), \quad (H_0^{(i)}, H_1^{(i)}) = (V_i, v_0U_i + 2u_0V_i).$$

Finally, note that it is obvious that the terms of these recurrence sequences are solutions of (2). Hence our claim follows. □

We shall also need a recent finiteness result of Bérczes et al. [2] concerning the number of terms of recurrence sequences representable as k-term sums of S-units.

Lemma 3.3. *Let U_n be a non-degenerate binary linear recurrence sequence as in (6), and suppose that the characteristic polynomial of U_n has irrational roots. Then for any fixed $k \geq 1$, Eq. (1) is solvable in $z_1, \ldots, z_k \in U_S$ at most for finitely many n. Further, the number of indices n for which (1) is solvable for this fixed k, can be bounded by an effectively computable constant depending only on ℓ and k.*

Proof. The statement is a simple consequence of [2, Theorem 1] and its proof. Note that the statement in [2] concerns only the case where $z_1, \ldots, z_k \in U_S \cap \mathbb{Z}$, however, from the proof it is clear that this more general formulation is also valid. □

Our last lemma is a deep result concerning the finiteness of the solutions of S-unit equations. For its formulation, we need to introduce some further notation.

Let $\mathbb{K}$ be an algebraic number field, and let $\mathcal{S} = \{P_1, \ldots, P_\ell\}$ be a finite set of prime ideals of $\mathbb{K}$. Write $U_{\mathcal{S}}$ for the $\mathcal{S}$-units in $\mathbb{K}$, that is, for the set of those $\alpha \in \mathbb{K}$ for which the principal fractional ideal (α) can be represented as

$$(\alpha) = P_1^{b_1} \cdots P_\ell^{b_\ell} \quad (b_1, \ldots, b_\ell \in \mathbb{Z}).$$

By the (naive) height $h(\gamma)$ of an element $\gamma \in \mathbb{K}$ we mean the maximum of the absolute values of the coefficients of the defining primitive polynomial of γ in $\mathbb{Z}[x]$. Note that for $\gamma \in \mathbb{Q}$, $h(\gamma)$ is just the maximum of the absolute values of the numerator and denominator of γ.

Lemma 3.4. *Use the above notation, and let $a_1,\dots,a_k$ be non-zero elements of $\mathbb{K}$. Then the equation*

$$a_1x_1+\cdots+a_kx_k=1 \tag{9}$$

has at most c_7 solutions $(x_1,\dots,x_k)\in U_{\mathcal{S}}^k$ for which the left hand side of (9) has no vanishing subsums. Here c_7 is an effectively computable constant depending only on k,ℓ, and $\deg\mathbb{K}$.

Further, if $k=2$, then we also have $\max(h(x_1),h(x_2))<c_8$, where c_8 is an effectively computable constant depending only on $a_1,a_2,\mathbb{K},\mathcal{S}$.

Proof. The statement follows from [7, Theorem 6.1.3, p. 132] and [7, Corollary 4.1.5, p. 65]. For the history of the equation and for related results, see [7]. □

Now we are ready to give the proof of Theorem 2.1.

Proof of Theorem 2.1. Let $z_1,\dots,z_k\in U_S$ satisfy (4) and (3). Assume first that

$$z_1+\cdots+z_k\in X.$$

Let (p,q) be a solution of (2) such that

$$z_1+\cdots+z_k=p,$$

and write $z=\gcd(p,q)$. Observe that $z\mid t$. By Lemma 3.2, we have that

$$z_1+\cdots+z_k=zG_n^{(i)} \tag{10}$$

with some $i\in\{1,\dots,I\}$ and $n\geq 0$, where I is bounded in terms of $\omega(t)$ and $G_n^{(i)}$ is a term of a non-degenerate binary recurrence sequence $G^{(i)}=G^{(i)}(2u_0,-1,G_0^{(i)},G_1^{(i)})$. Note that as $v_0>0$ (in Lemma 3.1), we have $u_0>1$. Thus the roots α and β of the characteristic polynomial

$$f(x)=x^2-2u_0+1$$

are (real) irrational numbers. (Observe that here $f(x)$, hence α and β are independent of i.) We can rewrite (10) as

$$z^{-1}z_1+\cdots+z^{-1}z_k=G_n^{(i)},$$

and observe that here $w_j:=z^{-1}z_j$ $(j=1,\dots,k)$ is an S^*-unit, where

$$S^*=S\cup\{p\text{ prime}:p\mid t\}.$$

Thus by Lemma 3.3, we see that the number of possible indices n in (10) is bounded by a constant c_9 depending only on ℓ, $\omega(t)$, and k. Further, by (3), $G_n^{(i)}\neq 0$ in (10). Thus setting $a_j=1/G_n^{(i)}$ for $j=1,\dots,k$, Eq. (10) can be rewritten as

$$a_1w_1+\cdots+a_kw_k=1.$$

Hence in view of (3), and as the number of the above type equations appearing is at most c_9, our statement concerning the number of solutions to (4) follows by Lemma 3.4. Further, in the particular case $k=1$, Eq. (10) reduces to

$$w_1=G_n^{(i)}, \tag{11}$$

which in view of Lemma 3.2 and (7) can be rewritten as

$$a_i\frac{\alpha^n}{w_1}+b_i\frac{\beta^n}{w_1}=1$$

with some a_i, b_i depending only on d, t, where

$$\alpha = u_0+\sqrt{d}v_0, \quad \beta = u_0-\sqrt{d}v_0.$$

Let

$$\mathcal{S}=\bigcup_{p\in S^*}\{P : P \text{ is a prime ideal in } \mathbb{Q}(\sqrt{d}),\ P|(p)\}.$$

As α and β are roots of the polynomial x^2-2u_0x+1, they are units in $\mathbb{Q}(\sqrt{d})$, so $\alpha, \beta \in U_{\mathcal{S}}$. Thus by Lemma 3.4, we obtain that for some $(\gamma_1,\gamma_2)\in U_{\mathcal{S}}\times U_{\mathcal{S}}$ with $\max(h(\gamma_1),h(\gamma_2))<c_{10}$, where c_{10} is a constant depending only on d, t, and S, we have

$$\frac{\alpha^n}{w_1}=\gamma_1, \quad \frac{\beta^n}{w_1}=\gamma_2.$$

By multiplying these expressions, in view of $\alpha\beta=1$, we obtain

$$w_1^2=\frac{1}{\gamma_1\gamma_2},$$

whence we can bound $h(z_1)$ in terms of d, t, and S. Hence in this case, our claim follows also for $k=1$.

Let now

$$z_1+\cdots+z_k\in Y.$$

In this case, a similar argument applies, using the sequences $H^{(i)}$ in place of the sequences $G^{(i)}$. Thus we omit the details, and the proof of the theorem is complete. □

Remark. In case of $t\in\{\pm1,\pm4\}$, one can easily check that the sequences $G^{(i)}$ and $H^{(i)}$ are Lucas-sequences of the first and second kind, respectively. Hence in this case, for $k=1$, in (11) (or in the equation $w_1=H_n^{(i)}$ when $z_1\in Y$), one can get a very good bound for n, using the famous result of Bilu, Hanrot, and Voutier [3] concerning the existence of primitive prime divisors of the terms of such sequences.

Acknowledgements. Open access funding provided by University of Debrecen (DE). The authors are indebted to the referee for the insightful remarks, which, in particular, helped to find the optimal formulation of Theorem 2.1 and Lemma 3.2 with respect to the dependence on the parameters involved.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

[1] Bertók, C., Hajdu, L., Pink, I., Rábai, Z.: Linear combinations of prime powers in binary recurrence sequences. Int. J. Number Theory **13**, 261–271 (2017)

[2] Bertók, C., Hajdu, L., Pink, I., Rout, S.S.: Sums of S-units in recurrence sequences. J. Number Theory **196**, 353–363 (2019)

[3] Bilu, Y., Hanrot, G., Voutier, P.M.: Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte. J. Reine Angew. Math. **539**, 75–122 (2001)

[4] Bravo, J.J., Faye, B., Luca, F.: Powers of two as sums of three Pell numbers. Taiwanese. J. Math. **21**, 739–751 (2017)

[5] Ddamulira, M., Luca, F.: On the x-coordinates of Pell equations which are k-generalized Fibonacci numbers. J. Number Theory **207**, 156–195 (2020)

[6] Erazo, H., Gómez, C. A., Luca, F.: Linear combinations of prime powers in X-coordinates of Pell equations. Ramanujan J. (to appear)

[7] Evertse, J.-H., Győry, K.: Unit Equations in Diophantine Number Theory, xv+363 pp. Cambridge University Press, Cambridge (2015)

[8] Guzman-Sanchez, S., Luca, F.: Linear combinations of factorials and S-units in a binary recurrence sequence. Ann. Math. Qué. **38**, 169–188 (2014)

[9] Győry, K.: On the numbers of families of solutions of systems of decomposable form equations. Publ. Math. Debr. **42**, 65–101 (1993)

[10] Liptai, K.: Pell egyenletek megoldása lineáris rekurzív sorozatok segítségével. Acta Acad. Paed. Agriensis Sect. Mat. **21**, 15–26 (1993)

[11] Luca, F., Togbé, A.: On the x-coordinates of Pell equations which are Fibonacci numbers. Math. Scand. **122**, 18–30 (2018)

[12] Niven, I., Zuckerman, H.S., Montgomery, H.L.: An Introduction to the Theory of Numbers, 5th edn. Wiley, Hoboken (1991)

[13] Schinzel, A.: On two theorems of Gelfond and some of their applications. Acta Arith. **13**, 177–236 (1967). Corrigendum: Acta Arith. **16**, 101 (1969/1970)

[14] Shorey, T.N., Tijdeman, R.: Exponential Diophantine Equations. Cambridge University Press, Cambridge (1986)

L. Hajdu and P. Sebestyén
University of Debrecen
Institute of Mathematics
P.O. Box 400
Debrecen 4002
Hungary
e-mail: hajdul@science.unideb.hu

P. Sebestyén
e-mail: sebestyen.peter@science.unideb.hu

Received: 26 February 2020