Monatshefte für Mathematik manuscript No.
(will be inserted by the editor)

A Hasse-type principle for exponential Diophantine equations over number fields and its applications

Csanád Bertók · Lajos Hajdu

Received: date / Accepted: date

Abstract In this paper we extend a conjecture (which is a variant of a classical conjecture of Skolem) to exponential Diophantine equations over algebraic number fields. On the one hand, using a generalization of a result of Erdős, Pomerance and Schmutz concerning 'small' values of Carmichael's λ function, we give strong support for the validity of the conjecture, both theoretically and numerically. On the other hand, we demonstrate the applicability of our method by finding all representations of powers of $2, 3, 5, 7$ as a sum of three balancing numbers. Note that this problem reduces to finding all solutions of certain exponential Diophantine equations over a number field.

Keywords Hasse-principle, conjecture of Skolem, exponential Diophantine equation, local method, explicit solution

Mathematics Subject Classification (2000) 11D61

Research supported in part by the Hungarian Academy of Sciences, the ÚNKP-17-3, New National Excellence Program of the Ministry of Human Capacities, the NKFIH grants K115479 and NK104208 and by 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.

Cs. Bertók
University of Debrecen, Faculty of Informatics
and the MTA-DE Research Group "Equations, Functions and Curves"
of the Hungarian Academy of Sciences and the University of Debrecen
4002, Debrecen, Egyetem tér 1.
P.O. Box 400 E-mail: bertok.csanad@inf.unideb.hu

L. Hajdu
University of Debrecen, Department of Mathematics
4002, Debrecen, Egyetem tér 1.
P.O. Box 400 E-mail: hajdul@science.unideb.hu

1 Introduction

Let $\mathbb{K}$ be an algebraic number field, and denote by $\mathcal{O}_{\mathbb{K}}$ its ring of integers. Let $\alpha_1,\dots,\alpha_k$, $\beta_{11},\dots,\beta_{1\ell},\dots,\beta_{k1},\dots,\beta_{k\ell}$ be non-zero elements of $\mathbb{K}$ and $\gamma\in\mathbb{K}$, and consider the exponential diophantine equation

$$\alpha_1\beta_{11}^{u_{11}}\dots\beta_{1\ell}^{u_{1\ell}}+\dots+\alpha_k\beta_{k1}^{u_{k1}}\dots\beta_{k\ell}^{u_{k\ell}}=\gamma \tag{1}$$

in integers $u_{11},\dots,u_{1\ell},\dots,u_{k1},\dots,u_{k\ell}$. Observe that here in fact we may assume that the unknowns u_{ij} are non-negative integers. Indeed, we may split (1) into several cases, replacing some of the β_{ij} by $1/\beta_{ij}$ to achieve this property. Further, if some β_{ij} is not in $\mathcal{O}_{\mathbb{K}}$, then we can write $\beta_{ij}=\beta'_{ij}/\beta''_{ij}$ with $\beta'_{ij},\beta''_{ij}\in\mathcal{O}_{\mathbb{K}}$. Then clearing the denominators, we obtain an equation of the form (1) again, where the β_{ij} are algebraic integers. Hence, from this point, unless it is stated otherwise, we shall always assume that all the β_{ij} are in $\mathcal{O}_{\mathbb{K}}$, and that the unknown exponents u_{ij} are all non-negative integers. (Also note that it is not a restriction that the number of terms in each summand of (1) is the same: the β_{ij}-s are allowed to be 1.)

Equation (1) has a vast literature and a long history. For $k=2$, using Baker's method one can bound the exponents $u_{11},\dots,u_{1\ell},u_{21},\dots,u_{2\ell}$ in an effective way; see e.g. results of Győry [15,16]. Prescribing some restrictive assumptions in case of $k=3,4$, the solutions can still be effectively determined (see e.g. results of Vojta [31] and Bennett [4]). As it is also long known, (1) has only finitely many solutions for any k for which the left hand side has no vanishing subsum. Further, the number of such solutions can be explicitly bounded in terms of k and ℓ (see e.g. [14], [2] and for several related results [13], [12], and the references given there).

In this paper we propose the following

Conjecture. Suppose that one of the following two properties hold:

(i) equation (1) has no solution in **integers** u_{ij} $(1\le i\le k, 1\le j\le\ell)$,

(ii) none of β_{ij} $(1\le i\le k, 1\le j\le\ell)$ is a proper unit (i.e. a unit different from roots of unity) in $\mathcal{O}_{\mathbb{K}}$, and equation (1) has no solution in non-negative integers u_{ij} $(1\le i\le k, 1\le j\le\ell)$.

Then there exists an ideal $\mathfrak{M}$ in $\mathcal{O}_{\mathbb{K}}$ such that the congruence

$$\alpha_1\beta_{11}^{u_{11}}\dots\beta_{1\ell}^{u_{1\ell}}+\dots+\alpha_k\beta_{k1}^{u_{k1}}\dots\beta_{k\ell}^{u_{k\ell}}\equiv\gamma \pmod{\mathfrak{M}} \tag{2}$$

has no solutions in non-negative integers u_{ij} $(1\le i\le k, 1\le j\le\ell)$.

The conjecture is a variant of a classical conjecture of Skolem [29]. In fact, the original formulation of Skolem is not completely precise. For an exact formulation we refer to [25], pp. 398–399. The conjecture predicts a Hasse-type principle for exponential Diophantine equations. Skolem's conjecture has been considered in several papers. here we only mention those of Schinzel [25–27], and Bartolome, Bilu and Luca [3] (see also the references therein).

Importantly, Theorem 2 of Schinzel [25] also implies that in case of $k = 1$ our conjecture is true.

We also mention that the Conjecture is an extension of a conjecture from [5], to the algebraic case. However, there a simpler assumption was sufficient: namely, it was enough to assume that (1) has no solutions in non-negative integers. Now we briefly explain why in this more general situation this condition is not sufficient.

Let $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, and consider the equation

$$(1+\sqrt{2})^u + (1+\sqrt{2})^v = 2\sqrt{2}.$$

As one can easily check, this equation has no solution in non-negative integers u, v. However, the corresponding congruence does have a solution modulo $\mathfrak{M}$, for any ideal $\mathfrak{M}$ in $\mathcal{O}_{\mathbb{K}}$. The reason is that the above equation has solutions in **integers**, e.g. $(u, v) = (1, -1)$. Since $1 + \sqrt{2}$ is a unit in $\mathcal{O}_{\mathbb{K}}$, we can find a positive integer t such that $(1 + \sqrt{2})^t \equiv 1 \pmod{\mathfrak{M}}$. Hence we get

$$(1+\sqrt{2}) + (1+\sqrt{2})^{t-1} \equiv 2\sqrt{2} \pmod{\mathfrak{M}}.$$

However, this phenomenon clearly occurs only if one of the numbers β_{ij} is a unit in $\mathcal{O}_{\mathbb{K}}$ - otherwise we may find some modulus $\mathfrak{M}$ such that none of the β_{ij} is invertible modulo $\mathfrak{M}$. Further, if β_{ij} is a root of unity, and its exponent u_{ij} is negative in some solution, then we may clearly replace u_{ij} by a positive integer, to obtain another solution. Thus altogether it seems that the conditions (i) and (ii) may be sufficient to guarantee the Conjecture to hold.

In this paper we give some theoretical and numerical evidence to support the Conjecture. First we prove that for any fixed α_i and β_{ij} $(1 \leq i \leq k, 1 \leq j \leq \ell)$, the set of $\gamma \in \mathcal{O}_{\mathbb{K}}$ for which the above Conjecture might fail, is 'very small'. For this, we shall use a generalization of a classical result of Erdős, Pomerance and Schmutz [10] concerning small values of Carmichael's λ function. We also support the Conjecture numerically, by checking its validity in different settings, and for a relatively large set of the parameters involved.

Further, based upon the Conjecture, we provide a method which is capable (at least heuristically) to find all solutions of equation (1), under certain assumptions. Interestingly, we are able to use the method also for some cases where neither of the conditions (i) and (ii) in the Conjecture is satisfied. We also mention that even if the Conjecture is not true for **all** equations, but holds for **some** equation, then our method is capable to provide all solutions of that equation (at least in principle). In fact the method is a generalization of that of [5] to the algebraic case. We mention that in the case where (1) is considered with $\mathbb{K} = \mathbb{Q}$, one can find several sparse results in the literature of this type (see [5] for related references). We demonstrate how our method works by finding all representations of powers of $2, 3, 5, 7$ as a sum of three balancing numbers. This problem reduces to finding all solutions of certain exponential Diophantine equations over a number field. Problems of this type are of wide recent interest; see e.g. the papers [6] and [8], and the references there. We describe the background of the problem and give further details in the corresponding subsection.

The structure of the paper is the following. In the next section we give our theoretical and numerical results supporting the Conjecture. Then we provide a method to find all solutions of exponential Diophantine equations over number fields, under some assumptions, and also give an application, by finding all representations of powers of $2, 3, 5, 7$ as a sum of three balancing numbers.

2 Results supporting the Conjecture

In this section we give our theoretical results, together with their proofs, and our numerical results supporting the Conjecture, in separate subsections.

2.1 Theoretical results

We start with a theorem which yields a good support for our Conjecture. As before, $\mathbb{K}$ denotes an algebraic number field, with ring of integers $\mathcal{O}_{\mathbb{K}}$. Further, for any subset L of $\mathcal{O}_{\mathbb{K}}$ and any ideal $\mathfrak{M}$ of $\mathcal{O}_{\mathbb{K}}$, write $L \pmod{\mathfrak{M}}$ for the natural embedding of the set L into $\mathcal{O}_{\mathbb{K}}/\mathfrak{M}\mathcal{O}_{\mathbb{K}}$. Finally, write $N(\mathfrak{M})$ for the norm of the ideal $\mathfrak{M}$ in $\mathcal{O}_{\mathbb{K}}$.

Theorem 1 *Let $\alpha_1, \dots, \alpha_k$, $\beta_{11}, \dots, \beta_{1\ell}, \dots, \beta_{k1}, \dots, \beta_{k\ell}$ be non-zero elements of $\mathcal{O}_{\mathbb{K}}$, and put*

$$H = \{\alpha_1 \beta_{11}^{u_{11}} \dots \beta_{1\ell}^{u_{1\ell}} + \dots + \alpha_k \beta_{k1}^{u_{k1}} \dots \beta_{k\ell}^{u_{k\ell}} : u_{ij} \in \mathbb{Z}\ (1 \le i \le k, 1 \le j \le \ell)\}.$$

Then for any ideal $\mathfrak{A}$ of $\mathcal{O}_{\mathbb{K}}$ and any $\varepsilon > 0$ there exists an ideal $\mathfrak{M}$ such that $\mathfrak{A} \mid \mathfrak{M}$, and $|H \pmod{\mathfrak{M}}| < N(\mathfrak{M})^{\varepsilon}$.

Remark 1. Choosing ε 'very small', the above theorem shows that it is 'very unlikely' that (1) is not solvable, but the corresponding congruence modulo $\mathfrak{M}$ is solvable. Since for any ε we can choose infinitely many $\mathfrak{M}$, this assertion seems to give a strong support for the Conjecture indeed.

Remark 2. The presence of $\mathfrak{A}$ is important to guarantee that some of the β_{ij} will not be invertible modulo $\mathfrak{M}$ (or even, we can make some β_{ij} be zero modulo $\mathfrak{M}$). This will be important later on, in applying the conjecture to find all solutions of (1) in the case where it does have solutions.

To give the proof of Theorem 1, we need some preparation. Let $\mathbb{K}$ be a number field, and $\mathcal{O}_{\mathbb{K}}$ be the ring of integers of $\mathbb{K}$. For an ideal $\mathfrak{I}$ in $\mathcal{O}_{\mathbb{K}}$, denote by $\varphi(\mathfrak{I})$ the number of invertible elements in $\mathcal{O}_{\mathbb{K}}/\mathfrak{I}$. Note that if $\mathbb{K} = \mathbb{Q}$, then the φ function is the same as Euler's totient function. The following lemma is a well-known property of the φ function; see e.g. Theorem 1.8 on p.21 of Narkiewicz [22].

Lemma 1 *Suppose that $\mathfrak{I}$ is an ideal in $\mathcal{O}_{\mathbb{K}}$ with $\mathfrak{I} = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_k^{n_k}$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ are distinct prime ideals in $\mathcal{O}_{\mathbb{K}}$. Then we have*

$$\varphi(\mathfrak{I}) = N(\mathfrak{p}_1)^{n_1-1} \cdots N(\mathfrak{p}_k)^{n_k-1}(N(\mathfrak{p}_1)-1)\cdots(N(\mathfrak{p}_k)-1),$$

where $N(\mathfrak{I})$ is the norm of $\mathfrak{I}$.

For any ideal $\mathfrak{I}$ in $\mathcal{O}_{\mathbb{K}}$, write

$$\lambda(\mathfrak{I}) := \text{lcm}\{\text{ord}_{\mathfrak{I}}(\alpha) \mid \alpha \in \mathcal{O}_{\mathbb{K}}\, , \alpha \text{ is invertible in } \mathcal{O}_{\mathbb{K}}/\mathfrak{I}\},$$

where $\text{ord}_{\mathfrak{I}}(\alpha)$ is the smallest positive integer t with $\alpha^t \equiv 1 \pmod{\mathfrak{I}}$. Note that if $\mathbb{K} = \mathbb{Q}$, then the λ function coincides with Carmichael's function. Obviously, for any ideal $\mathfrak{I}$, we have $\lambda(\mathfrak{I}) \mid \varphi(\mathfrak{I})$. Further, as it is well-known, see e.g. Laššák and Porubský [20], we have the following assertion.

Lemma 2 *Suppose that $\mathfrak{I}$ is an ideal in $\mathcal{O}_{\mathbb{K}}$ with $\mathfrak{I} = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_k^{n_k}$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ are distinct prime ideals in $\mathcal{O}_{\mathbb{K}}$. Then we have*

$$\lambda(\mathfrak{I}) = lcm(\lambda(\mathfrak{p}_1^{n_1}), \dots, \lambda(\mathfrak{p}_k^{n_k})).$$

We shall also need the following variant of a result of Erdős, Pomerance and Schmutz [10] concerning small values of Carmichael's function due to Pollack [24]. For other variants see e.g. [1], [17] and [5].

Lemma 3 *Let $\mathbb{K} = \mathbb{Q}$, and P be a set of primes of positive upper relative density. For each $\kappa > 0$, there are infinitely many square-free natural numbers n which are divisible only by primes in P and which satisfy $\lambda(n) < n^\kappa$.*

Combining the above lemmas with certain other assertions, we obtain the following property of the λ function defined over $\mathbb{K}$. Note that this result is a kind of extension of the above mentioned results concerning Carmichael's function over algebraic number fields.

Lemma 4 *For any $\delta > 0$ and ideal $\mathfrak{A}$ in $\mathcal{O}_{\mathbb{K}}$ there exists an ideal $\mathfrak{M}$ in $\mathcal{O}_{\mathbb{K}}$ such that $\mathfrak{A} \mid \mathfrak{M}$ and $\lambda(\mathfrak{M}) < N(\mathfrak{M})^\delta$.*

Proof To prove the statement, we closely follow arguments of Pollack [24], with small modifications. Let P be the set of those primes p which split completely in $\mathbb{K}$, such that (p) and $\mathfrak{A}$ are coprime ideals in $\mathcal{O}_{\mathbb{K}}$. It follows from Landau's prime ideal theorem [19] that P has positive upper density. Thus applying Lemma 3 with this set and some $\kappa > 0$, such that $\kappa < \delta d$, where d is the degree of $\mathbb{K}$, we obtain that there exists a positive integer n of the form $n = p_1 \dots p_k$ where $p_1, \dots, p_k$ are distinct primes from P, such that $\lambda(n) < n^\kappa$ and $N(\mathfrak{A})^{1-\delta} < n^{\delta d - \kappa}$. (Here and later on, $\lambda(n)$ is to be understood over $\mathbb{Q}$.) Write $\mathfrak{M} = (n)\mathfrak{A}$ with this n, and let $p_i = \mathfrak{p}_{i1} \dots \mathfrak{p}_{id}$ $(i = 1, \dots, k)$, where the $\mathfrak{p}_{ij}$ are prime ideals in $\mathbb{K}$. Then using Lemmas 1 and 2 we have

$$\lambda(\mathfrak{M}) \le \lambda(\mathfrak{A})\text{lcm}(\lambda(\mathfrak{p}_{11}), \dots, \lambda(\mathfrak{p}_{1d}), \dots, \lambda(\mathfrak{p}_{k1}), \dots, \lambda(\mathfrak{p}_{kd})) \le$$
$$\le \lambda(\mathfrak{A})\text{lcm}(\varphi(\mathfrak{p}_{11}), \dots, \varphi(\mathfrak{p}_{1d}), \dots, \varphi(\mathfrak{p}_{k1}), \dots, \varphi(\mathfrak{p}_{kd})) =$$
$$= \lambda(\mathfrak{A})\text{lcm}(p_1 - 1, \dots, p_k - 1) = \lambda(\mathfrak{A})\lambda(n) < N(\mathfrak{A})n^\kappa < N(\mathfrak{A})^\delta n^{\delta d} = N(\mathfrak{M})^\delta.$$

This proves the statement.

In fact, we shall need a statement which shows that for all $\alpha \in \mathcal{O}_{\mathbb{K}}$, the powers of α form a 'small' set modulo some $\mathfrak{M}$, and Lemma 4 guarantees this only for α with $\gcd((\alpha), \mathfrak{M}) = 1$. To get such a statement, observe that for any ideal $\mathfrak{I}$ in $\mathcal{O}_{\mathbb{K}}$ and $\alpha \in \mathcal{O}_{\mathbb{K}}$ with $\gcd((\alpha), \mathfrak{M}) = 1$, we have

$$\mathrm{ord}_{\mathfrak{I}}(\alpha) = \#\{\alpha^k \pmod{\mathfrak{I}} : k \in \mathbb{Z}\}.$$

We shall use the above notation for any $\alpha \in \mathcal{O}_{\mathbb{K}}$, and further write

$$L(\mathfrak{I}) = \max\{\mathrm{ord}_{\mathfrak{I}}(\alpha) \mid \alpha \in \mathcal{O}_{\mathbb{K}}\}.$$

Our next lemma will provide the necessary extension. Note that similar statements can be found in [1] and [5].

Lemma 5 *Let $\mathfrak{I} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_\ell^{n_\ell}$, and write $t = \max\{n_1, \ldots, n_\ell\}$. Then for all $\alpha \in \mathcal{O}_{\mathbb{K}}$ we have ord$_{\mathfrak{I}}(\alpha) \leq \lambda(\mathfrak{I}) + t$.*

Proof Write $(\alpha) = \mathfrak{q}_1^{u_1} \cdots \mathfrak{q}_r^{u_r} \cdot \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_\ell^{v_\ell}$, where the $\mathfrak{q}_i$ are prime ideals with $\mathfrak{q}_i \neq \mathfrak{p}_j$, and the exponents u_i, v_j are non-negative integers. We show that for any $x > \lambda(\mathfrak{I})$ there exists a y with $1 \leq y \leq \lambda(\mathfrak{I})$ such that $\alpha^{x+t} \equiv \alpha^{y+t} \pmod{\mathfrak{I}}$. Given x, choose a y with $1 \leq y \leq \lambda(\mathfrak{I})$ such that $\alpha^{x+t} \equiv \alpha^{y+t} \pmod{\mathfrak{I}'}$, where $\mathfrak{I}' = \prod\limits_{v_i=0} \mathfrak{p}_i^{n_i}$. Since $\gcd(\alpha, \mathfrak{I}') = 1$ and $\lambda(\mathfrak{I}') \leq \lambda(\mathfrak{I})$, such a y exists. Thus it remains only to prove that $\alpha^{x+t} \equiv \alpha^{y+t} \pmod{\mathfrak{I}''}$, where $\mathfrak{I}'' = \prod\limits_{v_i \neq 0} \mathfrak{p}_i^{n_i}$. Since $x, y \geq 0$, this statement is trivial.

Now we can give the proof of Theorem 1.

Proof (Proof of Theorem 1) Take a $\delta > 0$, and using Lemma 4, choose an ideal $\mathfrak{M}$ such that $\mathfrak{A} \mid \mathfrak{M}$ and $\lambda(\mathfrak{M}) < N(\mathfrak{M})^\delta$. Here (by choosing some appropriate ideal divisor $\mathfrak{B}$ of $\mathfrak{M}$) we may further assume that $N(\mathfrak{M})$ is so large that $N(\mathfrak{M})^\delta \geq \log(N(\mathfrak{M})$. Then, using Lemma 5, we get that

$$\mathrm{ord}_{\mathfrak{M}}(\alpha) \leq N(\mathfrak{M})^\delta + \log(N(\mathfrak{M}))/\log 2$$

for any $\alpha \in \mathcal{O}_{\mathbb{K}}$. Thus

$$|H \pmod{\mathfrak{M}}| \leq (N(\mathfrak{M})^\delta + \log(N(\mathfrak{M}))/\log 2)^{k\ell}.$$

Hence choosing δ appropriately, the theorem follows.

2.2 Numerical results supporting the Conjecture

In this section we give some numerical results to support the Conjecture. Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, where d is one of $2, 3, 5$ and consider the equations

$$\beta_1^{u_1} + 2\beta_2^{u_2} - 3\beta_3^{u_3} = 1, \qquad (3)$$

where $\beta_i = a_i + b_i\sqrt{d}$ such that a_i and b_i are integers with $\max\{|a_i|, |b_i|\} \leq 3$ and u_i is a non-zero integer for every $i = 1, 2, 3$. (We decided to exclude the case when one or more exponents are zero, since in those cases we can use e.g. Baker's method to handle the equations.) Taking everything into account we have $7^6 = 117649$ equations for every d.

Our goal is that for any equations (3) which is not solvable, give an ideal $\mathfrak{M}$ such that the equation has no solutions modulo $\mathfrak{M}$. Thus first we need to exclude all equations (3) which has a solution. For this, we do an exhaustive search for the exponent triple (u_1, u_2, u_3) in some large domain. Namely, we check the domain with $\max_{i=1,2,3} |u_i| \leq 100$. Note that if some β_i is a unit in $\mathcal{O}_{\mathbb{K}}$, then we have to check the negative values of u_i indeed. After this search we are rather sure that we have found all equations (3) which are solvable. (Note that obviously, at this point we cannot be sure that this is really the case - however, as we shall see later, our expectation is proved to be valid.) After this step, we use three ideals for $d = 2, 3, 5$ $(\mathfrak{M}_2, \mathfrak{M}_{2,3}, \mathfrak{M}_{2,3,5})$. These ideals are defined in the following way. Fixing d (and hence $\mathbb{K}$), $\mathfrak{M}_2$ is generated by those m ideals in $\mathcal{O}_{\mathbb{K}}$ which are prime ideals with norm less than 50 and $\varphi(m)$ has only 2 as a prime divisor.

We define the sets $\mathfrak{M}_{2,3}$ and $\mathfrak{M}_{2,3,5}$ similarly by simply expanding the list of possible prime divisors to $2, 3$ and to $2, 3, 5$, respectively. The use of these ideals is motivated by our approach: by collecting the mentioned generators, we get an ideal with 'small' λ-values.

We get that after using $\mathfrak{M}_2$, $\mathfrak{M}_{2,3}$ and $\mathfrak{M}_{2,3,5}$ most of the equations for which we did not find solutions at the first stage, are not solvable. To handle the remaining equations we extended the ideals M_2, $M_{2,3}$ and $M_{2,3,5}$ to be generated by primes in $\mathcal{O}_{\mathbb{K}}$ with the same property as before, but norm at most 150. By using these new ideals we were able to prove that none of the remaining equations have solutions.

We summarize our results in the Tables 1,2 and 3. We only work with the cases where we have not found solutions at the first stage. For example, for $d = 2$ out of the $7^6 = 117649$ possible equations we found that $92636+20725 = 113361$ has no solutions if the exponent is 'small'. Then 92636 out of them proved to be unsolvable modulo $\mathfrak{M}_2$, and the remaining 20725 are not solvable modulo $\mathfrak{M}_{2,3}$.

		Solved	Remaining
$\mathfrak{M}_2$	$N \leq 50$	92636	20725
	$N \leq 150$	92636	20725
$\mathfrak{M}_{2,3}$	$N \leq 50$	20173	552
	$N \leq 150$	20725	0
$\mathfrak{M}_{2,3,5}$	$N \leq 50$	530	22
	$N \leq 150$	–	–

Table 1 The results for $d = 2$

Summarizing our results, we were able to prove that those equations (3) which has no solutions, are unsolvable modulo some ideal.

		Solved	Remaining
$\mathfrak{M}_2$	$N \leq 50$	55223	58305
	$N \leq 150$	55223	58305
$\mathfrak{M}_{2,3}$	$N \leq 50$	57622	583
	$N \leq 150$	57801	504
$\mathfrak{M}_{2,3,5}$	$N \leq 50$	380	203
	$N \leq 150$	504	0

Table 2 The results for $d = 3$

		Solved	Remaining
$\mathfrak{M}_2$	$N \leq 50$	44184	72165
	$N \leq 150$	44184	72165
$\mathfrak{M}_{2,3}$	$N \leq 50$	56815	15350
	$N \leq 150$	71407	758
$\mathfrak{M}_{2,3,5}$	$N \leq 50$	15326	24
	$N \leq 150$	758	0

Table 3 The results for $d = 5$

3 A method for the explicit solution of exponential Diophantine equations over number fields and its application

In this section first we outline a method for finding all solutions to (1), then we apply our method to solve a problem related to balancing numbers and powers of $2, 3, 5, 7$.

3.1 A method for solving (1)

Consider equation (1). As a start, we mention that we may assume that none of the β_{ij}-s is a root of unity. Indeed, otherwise we can just split the original equation into subcases, according to the finitely many values of $\beta_{ij}^{u_{ij}}$. We shall also assume that (1) has no solutions yielding vanishing subsums. To find all solutions of equation (1), we make the following steps. (Some explanation is also given.)

(I) We compose a complete list of solutions to equation (1). (Since we know that (1) has only finitely many solutions, and as widely believed, these solutions are 'small', this can be done by an exhaustive search on some 'large' domain. (If some of the β_{ij} are units, we should not forget about checking negative exponents, too.) After this step heuristically we may be strongly confident that we do know all solutions of (1). The problem is how to prove it.)

(II) We choose one of the unknowns, u_{ij} say, belonging to some β_{ij} which is not a unit. Using the 'complete list' of solutions we take an integer u_0 with $u_{ij} < u_0$ in all known solutions. (As a variant of the method, at this point we could choose more exponents.)

(III) In place of equation (1), we consider the equation obtained by replacing the coefficient α_i with $\alpha_i\beta_{ij}^{u_0}$. (If our list of solutions is indeed complete, then the new equation has no solutions in non-negative integer exponents.)

(IV) We search for an $\mathfrak{M}$ such that the new equation has no solution modulo $\mathfrak{M}$. Having such an $\mathfrak{M}$, we can conclude that $u_{ij} < u_0$ holds for all solutions of (1). (If the Conjecture is true, then such a modulus exists. In our examples we shall show strategies how we try to find such an $\mathfrak{M}$. One method is based upon the proof of Theorem 1. As an important point, observe that for the unsolvability of the congruence modulo $\mathfrak{M}$ the relation we need to have $\mathfrak{A} := (\beta_{ij}^{u_0}) \mid \mathfrak{M}$ should hold, showing the importance of this property.)

(V) We split up the original equation into u_0 subcases according to the possible values of u_{ij}, and repeat the procedure for the new equations. (Observe that in the new equations we have one variable less.)

(VI) If everything works out well, then we are left with equations where all the remaining β_{ij} are units. We try to solve these equations with some other methods. (If there are no units among the β_{ij} or at most one of them is a unit, then we are done. If there are two units among the β_{ij}, we may apply Baker's method to find all solutions. There are also other cases where the problem becomes solvable: e.g. if all the remaining β_{ij}-s and the coefficients α_i are positive real numbers.)

Note that the method might also work if there are solutions yielding vanishing subsums: if there are terms which are not involved in such subsums, then the corresponding exponents may be bounded as above, and the final equation obtained can be solvable (e.g. by Baker's method, if the number of remaining terms is sufficiently reduced). We also mention that though the method is certainly heuristic, if we succeed to perform all steps, then finally we can find a complete list of solutions to (1), independently of any conjecture.

3.2 Sum of three balancing number yielding a power of $2, 3, 5, 7$

The sequence of balancing numbers $(B_n)_{n=0}^{\infty}$ is defined by $B_0 = 0$, $B_1 = 1$ and $B_{n+2} = 6B_{n+1} - B_n$ $(n \geq 0)$. That is, the sequence is a special Lucas-sequence. Problems related to balancing numbers have a vast literature; see e.g. the papers [18,21,23,30] and the references given there. We can write

$$B_n = \frac{\beta_1^n - \beta_2^n}{\beta_1 - \beta_2} \quad (n \geq 0),$$

where $\beta_1 = 3 + 2\sqrt{2}$ and $\beta_2 = 3 - 2\sqrt{2}$. Consider the following equation

$$B_u + B_v + B_w = b^z \tag{4}$$

in non-negative integers u, v, w, z, where $b \in \{2, 3, 5, 7\}$. Such equations (that is, representing powers as sums of terms of certain linear recurrence sequences) is of large recent interest, many papers deal with such questions. We refer e.g. to the papers [6,8,9] and the references given there. In these papers typically deep methods (such as Baker's method) are combined with certain reduction techniques (with the exception of [6], where an 'ad-hoc' local method is applied). Now we show that the approach suggested in the previous subsection, can also be capable (at least in principle) to handle such problems.

For this, let $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, and write (4) as

$$\beta_1^u - \beta_2^u + \beta_1^v - \beta_2^v + \beta_1^w - \beta_2^w = 4\sqrt{2}b^z. \tag{5}$$

To find all solutions, first we do an exhaustive search on the domain $\max(|u|, |v|, |w|, |z|) \leq 100$ to get all 'small' solutions. (Since both β_1 and β_2 are units in $\mathcal{O}_{\mathbb{K}}$, it is possible that (5) has solutions with negative values of u, v, w, as well.) We suspect that we in fact have found all solutions - we only need to show this. We obtained that in all solutions we got, we have

$$z \leq \begin{cases} 6, & \text{if } b = 2, \\ 1, & \text{if } b = 3, \\ 1, & \text{if } b = 5, \\ 1, & \text{if } b = 7. \end{cases} \tag{6}$$

Now we construct moduli (separately for the values $b = 2, 3, 5, 7$) which show that (6) in fact holds for **all** solutions to (5) (and (4)). Since the process is similar in all cases, we explain it in detail only for $b = 2$.

Since we can write $2 = (\sqrt{2})^2$ in $\mathbb{K}$, (5) can be reformulated as

$$\beta_1^u - \beta_2^u + \beta_1^v - \beta_2^v + \beta_1^w - \beta_2^w = (\sqrt{2})^{2z+5}.$$

Based upon (6) we suspect that here $z \leq 6$. If this is true, then the equation

$$\beta_1^u - \beta_2^u + \beta_1^v - \beta_2^v + \beta_1^w - \beta_2^w = 2^9(\sqrt{2})^{z'} \tag{7}$$

has no solution in integers u, v, w, z'. However, then by the Conjecture we should be able to find a modulus $\mathfrak{M}$ to show this. It turns out that the modulus appearing in Table 4 is appropriate for this purpose. Hence we have that $z \leq 6$ for **all** solutions to (4). The solutions with $z \leq 6$ can be easily listed. Following the same argument, we got that (6) is valid in each case $b = 2, 3, 5, 7$, for **all** solutions. The moduli used are given in Table 4.

b	Modulus
2	$2^9 \cdot 3 \cdot 17 \cdot 257 \cdot 7681$
3	$3^2 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \cdot 29 \cdot \sqrt{2} \cdot (1+3\sqrt{2}) \cdot$ $(7+2\sqrt{2}) \cdot (1+2\sqrt{2}) \cdot (1+4\sqrt{2})$
5	$5^2 \cdot 3 \cdot 11 \cdot 25 \cdot (1+4\sqrt{2}) \cdot \sqrt{2} \cdot (7+2\sqrt{2}) \cdot (1+2\sqrt{2})$
7	$7^2 \cdot (1+2\sqrt{2}) \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \cdot 29 \cdot 251 \cdot \sqrt{2}$ $\cdot (1+8\sqrt{2}) \cdot (1+3\sqrt{2}) \cdot (7+2\sqrt{2}) \cdot (1+7\sqrt{2}) \cdot (1+4\sqrt{2})$

Table 4 The moduli used for $b = 2, 3, 5, 7$

We got the moduli in Table 4 in the following way. First we put b^k in the moduli, where k are the bounds for z appearing in (6). This is an inevitable step, since we want to prove that our modified equation (see e.q. equation (7)) has no so solutions. After this step we tried to find numbers m such that $\lambda(m)$ is "small". For this we used an approach similar to what is written in [10]. Namely we searched for prime ideals $\mathcal{I}$ (either generated by a rational prime, or by a prime in $\mathcal{O}_{\mathbb{K}}$) such that $\varphi(\mathcal{I})$ is divisible by "small" rational primes only. This method however was not enough to handle equation (7), so we took a different approach. We tried to find rational primes p such that $p-1$ is divisible by a big power of b.

We summarize the results of our calculations in the following

Theorem 2 *All solutions to equation* (4) *are given in the following table*

b	u	v	w	z
2	0	1	1	1
2	1	1	2	3
3	1	1	1	1
7	0	1	2	1

Table 5 The results for equation (4)

Note on Theorem 2: at equation (6) we got different bounds for (5) than what can bee seen in the theorem above. The cause for this is that since α and β are units in $\mathcal{O}_{\mathbb{K}}$ we may have solutions (and in most cases we actually have) with negative exponents. But in Theorem 2 we only list the solutions for (4), hence we only need those where u, v and w are non-negative integers.

Acknowledgements The authors are grateful to the anonymous referee for her/his important comments and to K. Győry and R. Tijdeman for the fruitful discussions and useful advice.

References

1. Zs. Ádám, L. Hajdu, F. Luca, *Representing integers as linear combinations of S-units*, Acta Arith. **138**, 101–107 (2009).
2. F. Amoroso and E. Viada, *Small points on subvariaties of a torus*, Duke Math. J. **150**, 407–442 (2009).
3. B. Bartolome, Y. Bilu and F. Luca, *On the exponential local-global principle*, Acta Arith. **159**, 101–111 (2013).
4. M. Bennett, *Effective S-unit equations and a conjecture of Newman*, unpublished conference talk, Marseille-Luminy, 2010.
5. Cs. Bertók and L. Hajdu, *A Hasse-type principle for exponential Diophantine equations and its applications*, Math. Comp. **85**, 849–860 (2016).
6. Cs. Bertók, L. Hajdu, I. Pink, Zs. Rábai, *Linear combinations of prime powers in binary recurrence sequences*, Int. J. Number Theory. **13**, 261–271 (2017).
7. W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24**, 235–265 (1997).
8. K. C. Chim, I. Pink and V. Ziegler, *On a variant of Pillai's problem*, IJNT (to appear).
9. M. Ddamulira, F. Luca and M. Rakotomalala, *On a Problem of Pillai with Fibonacci Numbers and Powers of* 2, J. Indian Math. Soc. (to appear).

10. P. Erdős, C. Pomerance, E. Schmutz, *Carmichael's lambda function*, Acta Arithmetica **58.4**, 363–385 (1991).
11. J.-H. Evertse, *On sums of S-units and linear recurrences*, Compositio Math. **53**, 225–244 (1984).
12. J.-H. Evertse, K. Győry, *Unit Equations in Diophantine Number Theory*, pp. 378, Cambridge University Press, Cambridge (2015).
13. J.-H. Evertse, K. Győry, C. Stewart, R. Tijdeman, *S-unit equations and their applications*, New Advances in Transcendence Theory (A. Baker, ed.), 110–174, Cambridge University Press, Cambridge (1988).
14. J. H. Evertse, H. P. Schlickewei and W. M Schmidt, *Linear equations in variables which lie in a multiplicative group*, Annals of Math. **155** 807–836 (2002).
15. K. Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. **54**, 583–600 (1979).
16. K. Győry, *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queen's Papers in Pure and Appl. Math. **56** (1980).
17. L. Hajdu and R. Tijdeman, *Representing integers as linear combinations of powers*, Publ. Math. Debrecen **79** 461–468 (2011).
18. T. Kovács, K. Liptai and P. Olajos, *On (a, b)-balancing numbers*, Publ. Math. Debrecen **77**, 485–498 (2010).
19. E. Landau, *Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes*, Math. Ann. **56**, 645–670 (1903).
20. M. Laššák and Š. Porubský, *Fermat-Euler theorem in algebraic number fields*, J. Number Theory **60**, 254–290 (1996).
21. K. Liptai, F. Luca, Á. Pintér and L. Szalay, *Generalized balancing numbers*, Indag. Math. (N.S.) **20**, 87–100 (2009).
22. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, pp. 712, Springer-Verlag Berlin Heidelberg (2004).
23. G. K. Panda, *Sequence balancing and cobalancing numbers*, Fibonacci Quart. **45**, 265–271 (2008).
24. P. Pollack, *A simple proof of a theorem of Hajdu–Jarden–Narkiewicz*, Colloq. Math. (to appear).
25. A. Schinzel, *On power residues and exponential congruences*, Acta Arith. **27**, 397–420 (1975).
26. A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32**, 245–274 (1977).
27. A. Schinzel, *Addendum and corrigendum to the paper "Abelian binomials, power residues and exponential congruences", Acta Arith. 32(1977), pp. 245-274*, Acta Arith. **36**, 101–104 (1980).
28. T. N. Shorey, R. Tijdeman, *Exponential Diophantine Equations*, pp. 252, Cambridge University Press, Cambridge, (1986).
29. T. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlsbarkeit gewisser diophantischer Gleichungen*, Vid. akad. Avh. Oslo I 1937 nr 12.
30. Sz. Tengely, *Balancing numbers which are products of consecutive integers*, Publ. Math. Debrecen **83**, 197–205 (2013).
31. P. Vojta, *Integral Points on Varieties*, Dissertation, Harvard University, 1983.