MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

A HASSE-TYPE PRINCIPLE FOR EXPONENTIAL DIOPHANTINE EQUATIONS AND ITS APPLICATIONS

CSANÁD BERTÓK AND LAJOS HAJDU

Abstract. We propose a conjecture, similar to Skolem's conjecture, on a Hasse-type principle for exponential diophantine equations. We prove that in a sense the principle is valid for "almost all" equations. Based upon this we propose a general method for the solution of exponential diophantine equations. Using a generalization of a result of Erdős, Pomerance and Schmutz concerning Carmichael's λ function, we can make our search systematic for certain moduli needed in the method.

1. Introduction

Let $a_1, \dots, a_k$, $b_{11}, \dots, b_{1\ell}, \dots, b_{k1}, \dots, b_{k\ell}$ be non-zero integers, c be an integer, and consider the exponential diophantine equation

$$a_1 b_{11}^{\alpha_{11}} \dots b_{1\ell}^{\alpha_{1\ell}} + \dots + a_k b_{k1}^{\alpha_{k1}} \dots b_{k\ell}^{\alpha_{k\ell}} = c \tag{1.1}$$

in non-negative integers $\alpha_{11}, \dots, \alpha_{1\ell}, \dots, \alpha_{k1}, \dots, \alpha_{k\ell}$.

The effective and ineffective theory of (1.1) has a long history. In case of $k = 2$, one can apply Baker's method to give explicit bounds for the exponents $\alpha_{11}, \dots, \alpha_{1\ell}, \alpha_{21}, \dots, \alpha_{2\ell}$; see e.g. results of Győry [11, 12]. Note that by results of Vojta [23] and Bennett [6], the solutions to (1.1) can still be "effectively determined" for $k = 3, 4$, under some further restrictive assumptions. On the other hand, it is also known that for any k, the number of those solutions to equation (1.1) for which the left hand side of has no vanishing subsum is finite, and it can be bounded explicitly in terms of k and ℓ (see [10] and [4], and the references given there).

In this paper we propose the following

Conjecture. Suppose that equation (1.1) has no solutions. Then there exists an integer m with $m \geq 2$ such that the congruence

$$a_1 b_{11}^{\alpha_{11}} \dots b_{1\ell}^{\alpha_{1\ell}} + \dots + a_k b_{k1}^{\alpha_{k1}} \dots b_{k\ell}^{\alpha_{k\ell}} \equiv c \pmod{m} \tag{1.2}$$

has no solutions in non-negative integers $\alpha_{11}, \dots, \alpha_{1\ell}, \dots, \alpha_{k1}, \dots, \alpha_{k\ell}$.

The conjecture is a variant of a classical conjecture of Skolem [20]. Note that the original formulation of Skolem is not completely precise; for an exact formulation

2010 *Mathematics Subject Classification.* 11D61, 11D72, 11D79.

Key words and phrases. Exponential diophantine equations, Hasse-principle, Carmichael's function.

Research supported in part by the OTKA grants K100339 and NK101680, and by the TÁMOP-4.2.2.C-11/1/KONV-2012-0001 project. The project has been supported by the European Union, co-financed by the European Social Fund.

one should e.g. see [17], pp. 398–399. If true, then the conjecture can be considered as a Hasse-type principle for exponential diophantine equations. There are several results in the literature about Skolem's conjecture; we only mention theorems of Schinzel [17, 18, 19] and a recent paper of Bartolome, Bilu and Luca [5], and the references given there.

The results of Schinzel [17] also imply that in case of $k = 1$ our conjecture is true. In this paper first we show that for any fixed $a_1, \dots, a_k, b_{11}, \dots, b_{1\ell}, \dots, b_{k1}, \dots, b_{k\ell}$, the set of integers c for which the above conjecture fails, has density zero even inside the set of those values c for which equation (1.1) is not solvable. Moreover, here the appropriate moduli m can be chosen to have the extra property that they are all divisible by r, for any preliminary chosen integer r. The main tools in the proof are a generalization of a classical result of Erdős, Pomerance and Schmutz [9] concerning small values of Carmichael's λ-function, and a result of Ádám, Hajdu and Luca [1] about the number of values c up to any x, for which equation (1.1) is solvable. Further, we also give some "numerical evidence" for the conjecture, by checking its validity in different settings, and for a relatively large set of the parameters involved.

As an application, we present a general method for the solution of concrete equations of the type (1.1) under certain assumptions. Namely, if the Conjecture is true, then assuming that (1.1) has only finitely many solutions, our method makes it possible to find all these solutions. In fact the assumption about the finiteness of solutions can be relaxed. To illustrate the method, we present some concrete examples, as well.

We mention that in the literature one can find several sparse results of this type. For example, Alex, Brenner and Foster in a series of papers (see e.g. [8, 2, 3] and the references there) solved several equations of type (1.1), with typically $k = 4, 5$ and choices of $b_{11}, \dots, b_{1\ell}, \dots, b_{k1}, \dots, b_{k\ell}$ as small primes. We also mention related papers of Leitner [16] (where partially a result of Brenner and Foster [8] has been rediscovered) and Terai [22], where (beside among other general results) the exponential equation $(4m^2+1)^x + (5m^2-1)^y = (3m)^z$ is solved for fixed small values of m. However, in all these papers the way to find appropriate moduli like in (1.2) is rather ad-hoc, while in our method such moduli can be constructed systematically, based upon generalizations of arguments of Erdős, Pomerance and Schmutz [9].

We also note that in certain cases similar local arguments can be used to find all solutions for Diophantine equations of mixed polynomial-exponential type; see e.g. results and arguments of Leitner [16], Bennett, Bugeaud and Mignotte [7] and Hajdu and Pink [13], and the references given in these papers. However, the situations of polynomial-exponential equations and of purely exponential equations are drastically different. On the one hand, it is known that the local-global principle is not valid for polynomial-exponential equations in general. On the other hand, even if the principle is valid for a particular equation of this type, to find an appropriate modulus m one has to deal with additional problems. Namely, if say an n-th power occurs in the equation, then to build m, one should use primes p with $n \mid p-1$. For details, see the previously mentioned papers.

We have implemented our algorithm for the solution of exponential Diophantine equations in Sage [21]. The program, together with a complete description can be downloaded from the link www.math.unideb.hu/∼hajdul/expeqsolver.zip.

2. New results

In our first result we show that the Conjecture formulated in the Introduction is true for "almost all" cases. For the precise formulation, we need the following notion. If $A \subseteq B \subseteq \mathbb{Z}$ and B, then the density of A inside B is defined as

$$\lim_{x\to\infty} \frac{\#\{a \in A \ : \ |a| \le x\}}{\#\{b \in B \ : \ |b| \le x\}},$$

if the limit exists. Here and later on, $\#C$ denotes the number of elements of a set C.

Theorem 2.1. *Let $a_1, \dots, a_k$ and $b_{11}, \dots, b_{1\ell}, \dots, b_{k1}, \dots, b_{k\ell}$ be fixed, and let H be the set of right hand sides in* (1.1) *for which the Conjecture is violated, that is*

$$H = \{c \in \mathbb{Z} \ : \ (1.1) \text{ is not solvable, but } (1.2) \text{ is solvable for all } m\}.$$

Then H has density zero inside the set

$$H_0 = \{c \in \mathbb{Z} \ : \ (1.1) \text{ is not solvable}\}.$$

Note that Theorem 2.1 obviously implies that H has density zero inside $\mathbb{Z}$.

In the proof of Theorem 2.1 the following result plays an important role. This statement is a variant of a theorem of Erdős, Pomerance and Schmutz [9] and Hajdu and Tijdeman [14]. The important difference is the extra requirement that the appropriate moduli should be divisible by a fixed number r. This relation will play an important role in our method.

Let $\lambda(m)$ be the Carmichael function of the positive integer m, that is the least positive integer for which

$$b^{\lambda(m)} \equiv 1 \pmod{m}$$

for all $b \in \mathbb{Z}$ with $\gcd(b, m) = 1$. Later, we shall need the following information on small values of the Carmichael function.

Theorem 2.2. *There exist positive constants $C_1 > 1$ and C_2 such that for any integer r and for every large integer i there is an integer m with $r \mid m$, such that*

$$\log m \in [\log i + \log r, (\log i)^{C_1} + \log r]$$

and

$$\lambda(m) < r(\log m/r)^{C_2 \log\log\log m/r}.$$

Our next theorem provides numerical evidence for the Conjecture, for various settings.

Theorem 2.3. *Let c be an integer with $0 \le c \le 1000$. Then the Conjecture is valid for the following cases of equation* (1.1)*:*

1. $p_1^{\alpha_1} - p_2^{\alpha_2} = c$ *and* $p_1^{\alpha_1} + p_2^{\alpha_2} - p_3^{\alpha_3} = c$ *where p_1, p_2, p_3 are distinct primes less than* 100*,*
2. $p_1^{\alpha_1} + \cdots + p_{t-1}^{\alpha_{t-1}} - p_t^{\alpha_t} = c$ *where $p_1 < \cdots < p_t$ are primes less than* 30 *with $4 \le t \le 8$,*
3. $p_1^{\alpha_1} p_2^{\alpha_2} + p_3^{\alpha_3} p_4^{\alpha_4} - p_5^{\alpha_5} p_6^{\alpha_6} = c$ *where $p_1, p_2, p_3, p_4, p_5, p_6$ are the primes $2, 3, 5, 7, 11, 13$ in some order,*
4. $2^{\alpha_1} + 3^{\alpha_2} + 5^{\alpha_3} + 7^{\alpha_4} + 11^{\alpha_5} + 13^{\alpha_6} + 17^{\alpha_7} + 19^{\alpha_8} - 23^{\alpha_9} = 55191$.

Remark. The last equation in Theorem 2.3 has no solutions, but it has solutions if 55191 is replaced by any c with $0 \le c < 55191$.

3. The application of the Conjecture to the explicit solution of exponential diophantine equations

We propose the following principal strategy to find all solutions of equations of type (1.1). For the moment, for simplicity assume that the equation has only finitely many solutions. The question that under which settings the strategy may work, will be discussed later.

Principal strategy.

(I) Find the suspected list of all solutions to equation (1.1) through exhaustive search. [Note: Of course, at this point we cannot be sure that the list is complete. However, based upon the finiteness results concerning (1.1), heuristically we may be strongly confident about it.]

(II) Choose one of the unknowns, α_{ij} say, and based upon the suspected list of all solutions take an integer α_0 with $\alpha_{ij} < \alpha_0$. [Note: By choosing more than one unknown we can speed up the calculations in an obvious way. However, to keep the presentation at this point simple, we work only with one exponent.

(III) Instead of equation (1.1) consider the equation obtained by replacing the coefficient a_i with $a_i b_{ij}^{\alpha_0}$. [Note: If our suspected list contained all solutions to (1.1) indeed, then the new equation would have no solutions in non-negative integer exponents.]

(IV) Find an m such that the new equation has no solution modulo m. Having such an m, conclude that $\alpha_{ij} < \alpha_0$ holds for all solutions of (1.1). [Note: If the Conjecture is true, then such a modulus exists. One can try to construct an appropriate m using Theorem 2.2 (and its proof). Observe that for the unsolvability of the congruence modulo m the relation $r := b_{ij}^{\alpha_0} \mid m$ should hold, showing the importance of this property.]

Observe that though the strategy contains heuristic points, once we succeed to find an appropriate modulus m in the last step, it is justified that the original equation (1.1) has no solutions with $\alpha_{ij} \geq \alpha_0$. Hence we could get rid of an unknown, and we can repeat the whole procedure for an equation in one less variable than the original one. Finally, if everything works out well, we get all solutions.

This strategy works, at least in principle, if there exists a (not at all preliminary computable) constant A, such that for all solutions of (1.1) we have $\min_{1\leq i\leq k, 1\leq j\leq \ell} \alpha_{ij} < A$. (Since then we can eliminate one of the unknowns by the above method, etc.) This is the case, for example, if (1.1) has no solution with vanishing subsum.

At this point we mention that one can find in the literature several sparse results of this type; see e.g. the papers [8, 2, 3] and the references there. However, in these papers the appropriate moduli are found in a rather ad-hoc way, at least no clear strategy is explained to choose them. In our results we could use the moduli provided by Theorem 2.2. We give a detailed explanation in the proofs of our forthcoming theorems.

We illustrate our method by applying it to three branches of problems. In each case, we give two types of results. The first one always only shows that in the equations considered, one of the exponents can be bounded. To solve these equations completely one should iterate the method. The second type is where

this iteration is executed, and the complete solution of a particular equation is presented.

Our next result concerns the representation of $c = 0$ in (1.1) as sums and differences of powers of several distinct primes. Note that this result is closely related to a question of Brenner and Foster [8].

Theorem 3.1.

(1) *Let $3 \le t \le 6$ and let $p_1, \dots, p_t$ be distinct primes with $p_i \le 19$ $(i = 1, \dots, t)$. Then for the non-negative integer solutions $\alpha_1, \dots, \alpha_t$ of the equation*

$$p_1^{\alpha_1} + \cdots + p_{t-1}^{\alpha_{t-1}} - p_t^{\alpha_t} = 0$$

we have $\min\limits_{1 \le i \le t} \alpha_i \le 15$.

(2) *The equation*

$$3^{\alpha_1} + 5^{\alpha_2} + 11^{\alpha_3} + 13^{\alpha_4} + 17^{\alpha_5} - 19^{\alpha_6} = 0$$

has only two solutions in non-negative integers $\alpha_1, \dots, \alpha_6$, given by

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6) = (0, 1, 1, 0, 0, 1), (1, 0, 0, 1, 0, 1).$$

The following theorem concerns the case where all but one primes are equal. Obviously, in this case the exponents of these primes can be arranged in a non-decreasing way. Further, the smallest exponent must always be zero, that is why the constant 1 appears on the left hand side.

Theorem 3.2.

(1) *Let $3 \le t \le 9$ and let p, q be distinct primes with $p, q \le 19$. Then for the non-negative integer solutions $\alpha_1, \dots, \alpha_t$ of the equation*

$$1 + p^{\alpha_1} + \cdots + p^{\alpha_{t-1}} - q^{\alpha_t} = 0$$

we have $\min\limits_{1 \le i \le t} \alpha_i \le 6$.

(2) *The diophantine equation*

$$1 + 5^{\alpha_1} + 5^{\alpha_2} + 5^{\alpha_3} + 5^{\alpha_4} + 5^{\alpha_5} + 5^{\alpha_6} + 5^{\alpha_7} + 5^{\alpha_8} - 17^{\alpha_9} = 0$$

has only two solutions in non-negative integers $\alpha_1, \dots, \alpha_9$ with $\alpha_1 \le \cdots \le \alpha_8$, given by

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8, \alpha_9) =$$
$$= (0, 0, 0, 0, 0, 0, 1, 1, 1), (0, 0, 0, 1, 1, 2, 3, 3, 2).$$

Our final result concerns the case $\ell = 2$ in (1.1).

Theorem 3.3.

(1) *Let $p_1, \dots, p_6$ be distinct primes with $p_i \le 19$ $(i = 1, \dots, 6)$. Then for the non-negative integer solutions $\alpha_1, \dots, \alpha_6$ of the equation*

$$p_1^{\alpha_1} p_2^{\alpha_2} + p_3^{\alpha_3} p_4^{\alpha_4} - p_5^{\alpha_5} p_6^{\alpha_6} = 1$$

we have $\min\limits_{1 \le i \le 6} \alpha_i \le 5$.

(2) *The equation*

$$2^{\alpha_1} 3^{\alpha_2} + 5^{\alpha_3} 7^{\alpha_4} - 11^{\alpha_5} 13^{\alpha_6} = 1$$

has only two solutions in non-negative integers $\alpha_1, \dots, \alpha_6$, given by

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6) = (0, 0, 0, 0, 0, 0), (0, 2, 1, 0, 0, 1).$$

4. Proofs

We start with the proof of Theorem 2.2.

Proof of Theorem 2.2. Theorem 5 of [14] is just the statement with $r = 1$. So let C_1 and C_2 be the constants implied by Theorem 5 of [14], let r be an arbitrary positive integer, and let i be sufficiently large. Then by Theorem 5 of [14] there exists an n such that

$$\log n \in [\log i, (\log i)^{C_1}] \text{ and } \lambda(n) < (\log n)^{C_2 \log\log\log n}.$$

Put $m := rn$. Then obviously, $r \mid m$. Further, we immediately obtain

$$\log m \in [\log i + \log r, (\log i)^{C_1} + \log r].$$

Finally, as it is well-known, for any positive integers a, b we have $\lambda(ab) \leq a\lambda(b)$. Hence

$$\lambda(m) \leq r\lambda(n) < r(\log n)^{C_2 \log\log\log n} = r(\log m/r)^{C_2 \log\log\log m/r},$$

and the theorem follows. □

Now we continue with the proof of Theorem 2.1. For this, beside Theorem 2.2 we need the following results of Ádám, Hajdu and Luca [1].

Lemma 4.1. *Using the notation of Theorem 2.1, write $H_0(x)$ for the elements h of H_0 with $|h| \leq x$ where x is a positive real number. Then for all large x we have*

$$\#H_0(x) > 2x - C_3(\log x)^{C_4}$$

where C_3 and C_4 are constants depending only on the parameters k, a_i and b_{ij} occurring in (1.1)*.*

Proof. The statement is a simple consequence of Theorem 1 of [1]. □

We also need the following

Lemma 4.2. *Let $m = q_1^{\beta_1} \cdots q_z^{\beta_z}$ where $q_1, \ldots, q_z$ are distinct primes, $\beta_1, \ldots, \beta_z$ are positive integers, and let $b \in \mathbb{Z}$. Then we have*

$$\#\{b^u \pmod m : u \geq 0\} \leq \lambda(m) + \max_{1 \leq i \leq z} \alpha_i.$$

Proof. The statement is Lemma 1 in [1]. □

Now we are ready to prove Theorem 2.1.

Proof of Theorem 2.1. For a positive real number x set

$$H(x) := \{h \in H : |h| \leq x\} \quad \text{and} \quad H_0(x) := \{h \in H_0 : |h| \leq x\}.$$

We apply Lemmas 4.1 and 4.2, and Theorem 2.2 with $r = 1$ to prove our statement. Partly we follow the argument of Theorem 1 of [15]; see also the proof of Theorem 3 in [1].

Throughout the proof, we assume that x is large enough for the arguments to hold. By Theorem 2.2 we can choose an integer m, satisfying $m \leq \sqrt{x}$ and

$$\lambda(m) < (\log m)^{C_2 \log\log\log m}. \tag{4.1}$$

We may assume that m is the largest integer with these properties. Then by Theorem 2.2 we have that $m > f(x)$, with some monotone increasing function f of x, tending to infinity as x goes to infinity.

Let $m = q_1^{\beta_1} \cdots q_z^{\beta_z}$ be the prime factorization of m, where $q_1, \ldots, q_z$ are distinct primes and $\beta_1, \ldots, \beta_z$ are positive integers. Write $C(m)$ for the collection of the modulo m residue classes of those integers c for which the congruence (1.2) is solvable. Lemma 4.2 implies that we have

$$\#C(m) \le (\lambda(m) + \max_{1 \le i \le z} \beta_i)^{k\ell}. \tag{4.2}$$

On the other hand, by (4.1) we easily get that

$$\lambda(m) + \max_{1 \le i \le z} \beta_i \le (\log m)^{C_2 \log\log\log m} + \frac{\log m}{\log 2}. \tag{4.3}$$

Now by inequalities (4.2) and (4.3) we get that

$$\#C(m) < (\log m)^{C_5 \log\log\log m}, \tag{4.4}$$

where C_5 is a constant depending only on k and ℓ.

Write now $x = um + v$ where u is a positive integer and v is a non-negative real number with $v < m$. Observe that by our choice of m, u and v we have that

$$\log u \ge (\log(u+1))/2 \ge (\log x - \log m)/2 \ge (\log x)/4.$$

Let now ε be an arbitrary positive real number. Then the above inequality implies

$$\varepsilon x/3 \ge \varepsilon um/3 > m > v.$$

Further, we also have

$$\varepsilon x/3 > C_3(\log x)^{C_4}/2,$$

where C_3 and C_4 are given in Lemma 4.1. Finally, the lower bound $m > f(x)$ also gives

$$\varepsilon x/3 \ge \varepsilon um/3 > u(\log m)^{C_5 \log\log\log m}.$$

Thus, since by (4.4) and $x = um + v$ we have that

$$\#H(x) \le 2(u(\log m)^{C_5 \log\log\log m} + v) + 1,$$

the statement immediately follows by comparing the above inequality with

$$\#H_0(x) > 2x - C_3(\log x)^{C_4},$$

given by Lemma 4.1. □

Proof of Theorem 2.3. Since the proofs of the parts (1) to (4) are similar, we only give details in case of (3). Moreover, here we consider only the equations

$$2^{\alpha_1}3^{\alpha_2} + 5^{\alpha_3}7^{\alpha_4} - 11^{\alpha_5}13^{\alpha_6} = c \tag{4.5}$$

with $0 \le c \le 1000$. First, letting the exponents α_i $(i = 1, \ldots, 6)$ vary between 0 and 12, we find a list L (with $\#L = 224$) of c values for which we expect equation (4.5) not to have solutions. (Note that some equations in (3) have solutions with $\max_{1 \le i \le 6} \alpha_i = 12$.) At this stage, at least we are certain that for integers c with $0 \le c \le 1000$ not in the list L, equation (4.5) is solvable. Now we investigate the values $c \in L$ one by one. The smallest such value is $c = 11$, we shall work only with this, the others can be handled similarly. Take the modulus

$$m := 7031324575728 = 2^4 \cdot 3^2 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 97 \cdot 577.$$

(Later we shall explain how to find this m.) Now we could simply say that as one can easily check, equation (4.5) has no solutions modulo m. However, as this check is not that easy for some of the instances in (1) to (4), it is worth to do it in a

sophisticated way. (In particular, since the appropriate modulus m can be much larger than the one given above.)

First observe that all the factors of m have λ values composed exclusively of 2-s and 3-s. (This is the choice indicated by the proof of Erdős, Pomerance and Schmutz [9].) This makes it possible to combine the information obtained for the coefficients $\alpha_1, \dots, \alpha_6$ modulo the separate factors. (It is highly not economic to work with m as a modulus directly.) For example, modulo 2^4 we immediately get that $\alpha_1 = 0$ must hold, and we also get some congruence conditions for the other exponents, modulo a power of 2 (since the orders of all the factors modulo 2^4 are certainly powers of 2). Then, modulo 3^2 we get further conditions on α_3, α_4, α_5 and α_6, modulo $\mathrm{ord}_9(5) = 6$, $\mathrm{ord}_9(7) = 2$, $\mathrm{ord}_9(11) = 6$ and $\mathrm{ord}_9(13) = 3$, respectively. Finally, using all the factors of m as modulus, the resulting system of congruences obtained for the exponents $\alpha_1, \dots, \alpha_6$ proves to be non-solvable. This shows that equation (4.5) with $c = 11$ has no solutions modulo m indeed.

In all the other cases the proof goes along the same lines. In some cases one really needs to work with huge moduli. However, in all cases we encountered, the modulus

$$m^* = 2^4 \cdot 3^2 \cdot \prod_{\substack{p-1=2^u 3^v 5^w \\ 3<p<20000}} p$$

proved to be appropriate. That is, the m we found was always a divisor of m^*.

Finally, we explain how we found the appropriate moduli m. In fact the outlined procedure in many cases could be simplified, e.g. starting with a shorter list of prime powers.

Let M be the list of all prime power divisors of m^*. Consider an equation of the form

$$b_1^{\alpha_1} b_2^{\alpha_2} + b_3^{\alpha_3} b_4^{\alpha_4} - b_5^{\alpha_5} b_6^{\alpha_6} = c \tag{4.6}$$

(in all the other instances the procedure is similar). Define a heuristic measurement $f(t)$ for the "goodness" of the elements t of M, with respect to the bases $b_1, \dots, b_6$. We take the function $f(t)$ defined as

$$f(t) = o_1 o_2 o_3 o_4 o_5 o_6$$

where $o_i = \mathrm{ord}_t(b_i)$ $(i = 1, \dots, 6)$, with the convention $o_i = \mathrm{ord}_t(b_i) = 1$ if $\gcd(t, b_i) > 1$. Then we take the first t from M as modulus, for which $f(t)$ is minimal. By this modulus, we obtain some conditions for the exponents α_i modulo o_i $(i = 1, \dots, 6)$. In particular, if t is a power of the prime b_i, then we know that either α_i is smaller than the exponent of b_i in t, or $b_i^{\alpha_i} \equiv 0 \pmod{t}$.

For simplicity, suppose that $\gcd(b_i, t) = 1$ $(i = 1, \dots, 6)$ and that we have

$$\alpha_i \equiv \beta_i \pmod{o_i} \quad (i = 1, \dots, 6),$$

with some β_i subject to $0 \le \beta_i < o_i$. Then we can rewrite equation 4.6 as

$$a_1 (b_1')^{\gamma_1} (b_2')^{\gamma_2} + a_2 (b_3')^{\gamma_3} (b_4')^{\gamma_4} - a_3 (b_5')^{\gamma_5} (b_6')^{\gamma_6} = c$$

with

$$a_1 = b_1^{\beta_1} b_2^{\beta_2},\ a_2 = b_3^{\beta_1} b_4^{\beta_2},\ a_3 = b_5^{\beta_1} b_6^{\beta_2},$$

and

$$b_i' = b_i^{o_i},\ \gamma_i = (\alpha_i - \beta_i)/o_i\ (i = 1, \dots, 6).$$

Now we can apply the above method for this equation with M replaced by $M \setminus \{t\}$, etc. This way we could always guarantee that the next modulus t is the "best", which makes the computation relatively fast.

Note that all the necessary exponentiations can be made locally, which keeps the procedure economic. The calculations have been performed by the program package Sage [21]. □

Proof of Theorem 3.1. We only deal with the second statement, since it asserts the complete solution of an equation. Deriving an upper bound for one of the exponents will be a part of our method, so part (1) of the theorem can be proved in a similar way.

First, according to (I) of our Principal strategy, we find a suspected list of all solutions of the equation

$$3^{\alpha_1} + 5^{\alpha_2} + 11^{\alpha_3} + 13^{\alpha_4} + 17^{\alpha_5} - 19^{\alpha_6} = 0 \tag{4.7}$$

with $0 \le \alpha_1, \dots, \alpha_6 < 15$. We get only two solutions, namely

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6) = (0, 1, 1, 0, 0, 1), (1, 0, 0, 1, 0, 1).$$

So we strongly suspect that there are no other solutions. Now, following steps (II) and (III) of the strategy, but shifting the powers of all bases, we consider the equation

$$3^2 \cdot 3^{\alpha_1'} + 5^2 \cdot 5^{\alpha_2'} + 11^2 \cdot 11^{\alpha_3'} + 13^2 \cdot 13^{\alpha_4'} + 17 \cdot 17^{\alpha_5'} - 19^2 \cdot 19^{\alpha_6'} = 0.$$

If our list of two solutions is complete, then the above equation has no solutions in non-negative integers $\alpha_1', \dots, \alpha_6'$. To show this, we find a modulus m such that the congruence

$$3^2 \cdot 3^{\alpha_1'} + 5^2 \cdot 5^{\alpha_2'} + 11^2 \cdot 11^{\alpha_3'} + 13^2 \cdot 13^{\alpha_4'} + 17 \cdot 17^{\alpha_5'} - 19^2 \cdot 19^{\alpha_6'} \equiv 0 \pmod{m}$$

has no solutions. By a similar strategy as in the proof of Theorem 2.3, we find that

$$m = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 109 \cdot 163 \cdot 433$$

is an appropriate modulus. This means that in any solution of (4.7), one of

$$\alpha_1 \le 1, \quad \alpha_2 \le 1, \quad \alpha_3 \le 1, \quad \alpha_4 \le 1, \quad \alpha_5 = 0, \quad \alpha_6 \le 1$$

must be valid. This means that one of the exponents $\alpha_1, \dots, \alpha_6$ is fixed, and may take at most two values. We consider only the possibility $\alpha_1 = 0$, the other cases can be treated similarly. In this case our equation reads as

$$1 + 5^{\alpha_2} + 11^{\alpha_3} + 13^{\alpha_4} + 17^{\alpha_5} - 19^{\alpha_6} = 0.$$

Based upon our previous calculations, we suspect that this new equation has the only solution

$$(\alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6) = (1, 1, 0, 0, 1).$$

Now similarly as above, but shifting only the exponent of 13, if the conjecture is true, then there exists a modulus m such that the congruence

$$1 + 5^{\alpha_2} + 11^{\alpha_3} + 13 \cdot 13^{\alpha_4'} + 17^{\alpha_5} - 19^{\alpha_6} \equiv 0 \pmod{m}$$

has no solutions modulo m. Now by the same method as previously, we get that the modulus

$$m = 2^4 \cdot 3^2 \cdot 7 \cdot 13 \cdot 37 \cdot 73 \cdot 109 \cdot 433$$

verifies this assertion. Hence we obtain that $\alpha_4 = 0$ must be valid, and our equation reduces to

$$2 + 5^{\alpha_2} + 11^{\alpha_3} + 17^{\alpha_5} - 19^{\alpha_6} = 0.$$

By our earlier calculations, we strongly suspect that this equation has the only solution

$$(\alpha_2, \alpha_3, \alpha_5, \alpha_6) = (1, 1, 0, 1).$$

Shifting now the exponent of 17 by one, the modulus

$$m = 2 \cdot 3 \cdot 7 \cdot 17 \cdot 37 \cdot 73 \cdot 97 \cdot 109 \cdot 163$$

witnesses that the equation arising has no solutions - in other words, we must have $\alpha_5 = 0$.

Hence we obtain the equation

$$3 + 5^{\alpha_2} + 11^{\alpha_3} - 19^{\alpha_6} = 0,$$

with the only expected solution

$$(\alpha_2, \alpha_3, \alpha_6) = (1, 1, 1).$$

Now we shift the exponent of 5 to get the equation

$$3 + 5^2 \cdot 5^{\alpha_2'} + 11^{\alpha_3} - 19^{\alpha_6} = 0,$$

which turns out to have no solutions modulo

$$m = 3^3 \cdot 5^2 \cdot 7 \cdot 31.$$

This leaves us with the equations

$$4 + 11^{\alpha_3} - 19^{\alpha_6} = 0 \quad \text{and} \quad 8 + 11^{\alpha_3} - 19^{\alpha_6} = 0.$$

The first equation has no solutions modulo 3. Further, we suspect that the only solution of the second equation is

$$(\alpha_3, \alpha_6) = (1, 1).$$

Now we shift the exponent of 11 to obtain the equation

$$8 + 11^2 \cdot 11^{\alpha_3'} - 19^{\alpha_6} = 0,$$

which has no solutions modulo

$$m = 5^2 \cdot 11^2 \cdot 31 \cdot 61.$$

This means that $\alpha_3 = 0$ or $\alpha_3 = 1$. From this we easily get that $\alpha_3 = \alpha_6 = 1$ must be valid. By following similar arguments, we could solve all the encountered equations and we get that the solutions are those listed in the statement. □

Proof of Theorem 3.2. The proof of this theorem is very similar to that of Theorem 3.1, so we only indicate the main steps. Again, we only deal with part (2) of the statement, part (1) could be handled similarly.

After finding the suspected solutions

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8, \alpha_9) =$$

$$= (0, 0, 0, 0, 0, 0, 1, 1, 1), (0, 0, 0, 1, 1, 2, 3, 3, 2),$$

using the modulus

$$m = 2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601$$

we successively get $\alpha_1 = \alpha_2 = \alpha_3 = 0$ and $\alpha_4 \leq 1$.

In case of $\alpha_4 = 0$, using again m we successively obtain $\alpha_5 = \alpha_6 = 0$ and $\alpha_7 = \alpha_8 = 1$, whence $\alpha_9 = 1$, and we obtain the first solution calculated preliminary. Note that in some of the above arguments, m could be replaced by $m/5$ or $m/601$.

When $\alpha_4 = 1$, a similar calculation (but with rather more complicated moduli) leads to the second solution, and the theorem follows. □

Proof of Theorem 3.3. Again, we only deal with part (2) of the statement. Since the proof is very similar to the previous ones, we only give the moduli used, and the information deduced for the exponents.

We start with the equation

$$2^{\alpha_1}3^{\alpha_2} + 5^{\alpha_3}7^{\alpha_4} - 11^{\alpha_5}13^{\alpha_6} = 1.$$

Then modulo 2 we get that $\alpha_1 = 0$. So the equation reduces to

$$3^{\alpha_2} + 5^{\alpha_3}7^{\alpha_4} - 11^{\alpha_5}13^{\alpha_6} = 1.$$

Now taking

$$m = 2^5 \cdot 7 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 97 \cdot 193$$

we obtain that $\alpha_4 = 0$. Then our equation takes the form

$$3^{\alpha_2} + 5^{\alpha_3} - 11^{\alpha_5}13^{\alpha_6} = 1.$$

Taking

$$m = 7 \cdot 11 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 73 \cdot 97 \cdot 193$$

we get that $\alpha_5 = 0$, that is, we have to solve

$$3^{\alpha_2} + 5^{\alpha_3} - 13^{\alpha_6} = 1.$$

This equation modulo

$$m = 5^2 \cdot 7 \cdot 11 \cdot 31 \cdot 41$$

yields that $\alpha_3 \leq 1$. The equality $\alpha_3 = 0$ trivially leads to $\alpha_2 = \alpha_6 = 0$. This gives the first solution. So we are left with the case $\alpha_3 = 1$, when the equation is of the shape

$$3^{\alpha_2} - 13^{\alpha_6} = -4.$$

Then modulo

$$m = 27 \cdot 7 \cdot 19 \cdot 37$$

we get that $\alpha_2 \leq 2$, which easily yields $\alpha_2 = 2$ and $\alpha_6 = 1$. Thus we get the second solution, and the theorem follows. □

5. Acknowledgements

The authors are grateful to the referees for their helpful and valuable comments.

References

1. Zs. Ádám, L. Hajdu and F. Luca, *Representing integers as linear combinations of S-units*, Acta Arith. **138** (2009), 101–107.
2. L. J. Alex and L. L. Foster, *On the diophantine equation* $1 + x + y = z$, Rocky Mountain J. Math. **22** (1992), 11–62.
3. L. J. Alex and L. L. Foster, *On the diophantine equation* $w + x + y = z$, *with* $wxyz = 2^r 3^s 5^t$, Revista Mat. Univ. Comp. Madrid **8** (1995), 13–48.
4. F. Amoroso and E. Viada, *Small points on subvariaties of a torus*, Duke Math. J. **150** (2009), 407–442.
5. B. Bartolome, Y. Bilu and F. Luca, *On the exponential local-global principle*, Acta Arith. **159** (2013), 101–111.

6. M. Bennett, *Effective S-unit equations and a conjecture of Newman*, unpublished conference talk, Marseille-Luminy, 2010.
7. M. A. Bennett, Y. Bugeaud, M. Mignotte, *Perfect powers with few binary digits and related Diophantine problems, II*, Math. Proc. Camb. Phil. Soc. **153** (2012), 525–540.
8. J. L. Brenner and L. L. Foster, *Exponential diophantine equations*, Pacific J. Math. **101** (1982), 263–301.
9. P. Erdős, C. Pomerance and E. Schmutz, *Carmichael's lambda function*, Acta Arith. **58** (1991), 365–385.
10. J. H. Evertse, H. P. Schlickewei and W. M Schmidt, *Linear equations in variables which lie in a multiplicative group*, Annals of Math. **155** (2002), 807–836.
11. K. Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. **54** (1979), 583–600.
12. K. Győry, *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queen's Papers in Pure and Appl. Math. **56** (1980).
13. L. Hajdu and I. Pink, *On the Diophantine equation* $1 + 2^a + x^b = y^n$, J. Number Theory **143** (2014), 1–13.
14. L. Hajdu and R. Tijdeman, *Representing integers as linear combinations of powers*, Publ. Math. Debrecen **79** (2011), 461–468.
15. L. Hajdu and R. Tijdeman, *Representing integers as linear combinations of power products*, Archiv der Math. **98** (2012), 527–533.
16. D. J. Leitner, *Two exponential diophantine equations*, J. Théor. Nomb. Bordeaux **23** (2011), 479–487.
17. A. Schinzel, *On power residues and exponential congruences*, Acta Arith. **27** (1975), 397–420.
18. A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), 245–274.
19. 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** (1980), 101–104.
20. T. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlsbarkeit gewisser diophantischer Gleichungen*, Vid. akad. Avh. Oslo I 1937 nr 12.
21. W. A. Stein et al., *Sage Mathematics Software (Version 6.1.1)*, The Sage Development Team, 2014, http://www.sagemath.org.
22. N. Terai, *On the Exponential Diophantine Equation* $(4m^2+1)^x + (5m^2-1)^y = (3m)^z$, Int. J. Algebra **6** (2012), 1135–1146.
23. P. Vojta, *Integral Points on Varieties*, Dissertation, Harvard University, 1983.

Institute of Mathematics, University of Debrecen, H-4010 Debrecen, P.O. Box 12, Hungary

E-mail address: bertok.csanad@science.unideb.hu

Institute of Mathematics, University of Debrecen, H-4010 Debrecen, P.O. Box 12, Hungary

E-mail address: hajdul@science.unideb.hu