Dominik J. LEITNER

Two exponential diophantine equations

<http://jtnb.cedram.org/item?id=JTNB_2011__23_2_479_0>
Two exponential diophantine equations

par DOMINİK J. LEITNER

1. Introduction

In this note we find all solutions of the equation

\[ 3^a + 5^b - 7^c = 1 \]  

in non-negative integers \( a, b, c \), and also all solutions of the equation

\[ y^2 = 3^a + 2^b + 1. \]

in integers \( y \) and non-negative integers \( a, b \).

The equation (1.1) has been mentioned by Masser [M] (p. 203) as an example for which there is still no algorithm to solve completely. It can be interpreted as a special case of an \( S \)-unit equation, or, in a broader context, an equation of the type covered by the classical results of Mordell-Lang type. The structure of the solution set can be determined using the Subspace Theorem applied to the more general \( S \)-unit equation

\[ x_0 + x_1 + \cdots + x_n = 0 \]
in non-zero rational integers $x_0, x_1, \ldots, x_n$ with no common factor. When these integers are composed of primes from a fixed finite set, the consequence is that (1.3) has at most finitely many solutions satisfying

$$\sum_{i \in I} x_i \neq 0$$

for all non-empty subsets $I$ of $\{1, \ldots, n\}$. This (1.4) in our case (1.1) is hardly any restriction, and one finds at once that the solution set of (1.1) is at most finite. The general theory also provides an explicit estimate for the number of solutions. But the recent Theorem 1 (p.808) of the paper [ESS] of Evertse, Schlickewei and Schmidt gives only the upper bound $\exp(4.18^9) \approx 10^{34458538964}$, which is little use in actually finding the solutions. The same can be said even for the very recent improvement $24^{1944} \approx 10^{2683}$ by Amoroso and Viada [AV]. And it is notorious that in general there are no effective estimates at all for the sizes of the solutions of (1.3). Here we will use a relatively simple method of congruences to show that the only solutions are in fact $a = b = c = 0$ and $a = b = c = 1$.

The equation (1.2) has been mentioned by Zannier [Z1] (pp.61,62) and [Z2] (p.1) and Corvaja and Zannier [CZ2] (p.296), [CZ3] (pp.168,169) (see also [Z3] (p.434), [CZ1] and [C] (p.130)) in the context of the Lang-Vojta Conjecture (see for example [HS] (p.486)). Here the term $y^2$ prevents the use of the Subspace Theorem as above. And indeed they remark that it is not even known whether the solution set is finite or not, unless one assumes such a conjecture. One can also assume a version for (1.3) which was formulated in elementary terms by Vojta [V] (p.7). Namely, for every $\lambda > 1$ there is a constant $C$ and a non-zero homogeneous polynomial $F$, each depending only on $n$ and $\lambda$, such that all solutions of (1.3) in coprime integers satisfy

$$\max\{|x_0|, |x_1|, \ldots, |x_n|\} \leq CP^\lambda$$

where $P$ is the product of all the primes dividing the $x_0, x_1, \ldots, x_n$; however (1.4) now has to be replaced by

$$F(x_1, \ldots, x_n) \neq 0.$$  

For $n = 2$ this is of course the intractable $abc$-conjecture.

With (1.2) we get at once $y^2 \leq C(6|y|)^\lambda$ in (1.5) and so it suffices to fix $\lambda < 2$. Now the failure of (1.6) is not so trivial; but (with $x_0 = y^2$) it would lead to a point $(x_1, x_2) = (3^a, 2^b)$ on one of a finite set of fixed curves. Now since 3 and 2 are multiplicatively independent a well-known result of Liardet (see for example Theorem 7.3 (p.207) of [L]) implies that there are at most finitely many such points unless $x_1$ or $x_2$ is constant on one of the curves. But when $a$ or $b$ is constant in (1.2) then it is easy to establish the finiteness, for example with $n = 2$ in Vojta’s Conjecture.
Thus \textit{a fortiori} there is no algorithm for the complete solution. Nevertheless we will use the same congruence method to show that the set is indeed finite and in fact that the only solutions are $y = \pm 2, a = 0, b = 1$ and $y = \pm 6, a = 1, b = 5$ and $y = \pm 6, a = b = 3$.

Because both equations do actually have solutions, it may seem impossible that we can use congruences to prove the finiteness. And indeed it would be impossible for equations that are polynomial in all the variables. Here we have exponential terms like $3^a$. The values of this for example modulo $12$ at $a = 0, 1, 2, 3, 4, \ldots$ are $1, 3, 9, 3, 9, \ldots$; of course eventually periodic but not at once. So if we can show that $3^a$ must be $1$ modulo $12$, then we deduce $a = 0$ and not just a congruence for $a$. It is this principle that we shall exploit, for various moduli the largest of which is $1820$. In fact the various moduli could be taken together to show that we get no more solutions of (1.1) modulo $27927900$ (and even $20475$); however this kind of simplification seems not to be possible for (1.2).

Of course our method is far too special to be considered as a contribution to the theory of either the $S$-unit equation or the Vojta Conjecture. See also the remark in the footnote of \cite{Z1} (p.57). But its success with the fairly natural equations (1.1) and (1.2) perhaps gives hope that it can be applied to other interesting equations of the same sort. This is certainly true of $y^2 = 10^a + 6^b + 1$ also mentioned in \cite{Z1} (p.60), for example; and already there the same is noted for the two-variable equation $y^2 = 5^a + 2^a + 7$.

I am grateful to David Masser for advice on the preparation of this note. After it was submitted for publication, Michael Bennett kindly drew my attention to the article \cite{BF} of Brenner and Foster; it turns out that they had already proved our Theorem 2.1 about (1.1). However they considered nothing like (1.2).

2. The equation $3^a + 5^b - 7^c = 1$

In this section we prove the following result.

\textbf{Theorem 2.1.} Let $a, b, c$ in $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ satisfy (1.1); then either $a = b = c = 0$ or $a = b = c = 1$.

\textit{Proof.} We need one simple observation.

\textbf{Lemma 2.1.} Let $a, b, c$ be in $\mathbb{N}_0$ with (1.1) and $abc = 0$; then $a = b = c = 0$.

\textit{Proof.} At first let $a = 0$. Then (1.1) appears as $5^b = 7^c$ which forces $b = c = 0$. Similarly if we start with $b = 0$. Finally, $c = 0$ leads to $3^a + 5^b = 2$ and so again $a = b = c = 0$, which completes the proof of the present lemma. \hfill \Box

Lemma 2.1 shows that either $a = b = c = 0$ or $a, b, c \in \mathbb{N}$ and hence in the following we may assume $a, b, c \in \mathbb{N}$.
Let us consider the following table, where we calculate values of \(3^n, 5^n, 7^n\) modulo 1820

\[
\begin{array}{c|cccccccc}
 n & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
3^n \pmod{1820} & 3 & 9 & 27 & 81 & 243 & 729 & 367 \\
5^n \pmod{1820} & 5 & 25 & 125 & 625 & 1305 & 1065 & 1685 \\
7^n \pmod{1820} & 7 & 49 & 343 & 581 & 427 & 1169 & 903 \\
\end{array}
\]

\[
\begin{array}{c|cccccccc}
 n & 8 & 9 & 10 & 11 & 12 & 13 \\
3^n \pmod{1820} & 1101 & 1483 & 809 & 607 & 1 & 3 \\
5^n \pmod{1820} & 1145 & 265 & 1325 & 1165 & 365 & 5 \\
7^n \pmod{1820} & 861 & 567 & 329 & 483 & 1561 & 7 \\
\end{array}
\]

Here we get the same values for \(n = 1\) and \(n = 13\), hence we see a period of length 12 when we calculate the table above for all \(n\) in \(\mathbb{N}\).

Now, for \(m, k\) in \(\mathbb{N}_0\) we define \(\{m\}_k = m + k\mathbb{N}_0\). Then the values of \(n\) for which the triple \((3^n, 5^n, 7^n)\) lies in various congruence classes modulo 1820 form subsets \(\{1\}_{12}, \ldots, \{11\}_{12}\) of \(\mathbb{N}\).

Perhaps with the help of a computer we now look for \((a, b, c)\) with \(1 \leq a, b, c \leq 12\) such that

\[
3^a + 5^b - 7^c \equiv 1 \pmod{1820}.
\]

In fact we find that \((a, b, c) = (1, 1, 1)\) is the only triple as required and this proves that \(a, b, c\) lie in the set \(\{1\}_{12}\), which means that

\[
(2.1) \quad a \equiv b \equiv c \equiv 1 \pmod{12}.
\]

However, we rerun the procedure above modulo 341. Due to (2.1) we just consider values with \(n \equiv 1 \pmod{12}\) and get the table

\[
\begin{array}{c|ccccccc}
 n & 1 & 13 & 25 & 37 & 49 & 61 \\
3^n \pmod{341} & 3 & 148 & 254 & 141 & 136 & 3 \\
5^n \pmod{341} & 5 & 191 & 67 & 36 & 284 & 5 \\
7^n \pmod{341} & 7 & 112 & 87 & 28 & 107 & 7 \\
\end{array}
\]

Here we see a period of length 60 and, as before, we find that \((1, 1, 1)\) is the only solution of (1.1) modulo 341 from the table above. This implies that

\[
a \equiv b \equiv c \equiv 1 \pmod{60}.
\]

Let us continue with the following table modulo 50

\[
\begin{array}{c|ccc}
 n & 1 & 61 & 121 \\
3^n \pmod{50} & 3 & 3 & 3 \\
5^n \pmod{50} & 5 & 25 & 25 \\
7^n \pmod{50} & 7 & 7 & 7 \\
\end{array}
\]
Two exponential diophantine equations

Here we have only the two classes \( \{1\}_0 = \{1\} \) and \( \{61\}_{60} \), in which the first class is finite because the sequence \( 5^n \pmod{50} \) is not periodic but only eventually so. Now looking for solutions of (1.1) modulo 50 forces \( b = 1 \).

Thus with (1.1) we get the new equation

\[
7^c - 3^a = 4.
\]

And here

<table>
<thead>
<tr>
<th>( n )</th>
<th>1</th>
<th>61</th>
<th>121</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 7^n \pmod{9} )</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>( 3^n \pmod{9} )</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

which forces in a similar way \( a = 1 \). Now (2.2) implies that \( c = 1 \) and this completes the proof of Theorem 2.1. \( \square \)

3. The equation \( y^2 = 3^a + 2^b + 1 \)

In this section we prove the following result.

**Theorem 3.1.** Let \( y \in \mathbb{Z} \) and \( a, b \in \mathbb{N}_0 \) satisfy (1.2); then either \( y = \pm 2 \) and \( a = 0, b = 1 \) or \( y = \pm 6 \) and \( a = 1, b = 5 \) or \( a = b = 3 \).

At first we note that \( y \neq 0 \) and hence we may assume \( y \in \mathbb{N} \) without loss of generality.

**Lemma 3.1.** Let \( y \in \mathbb{N} \) and \( a, b \in \mathbb{N}_0 \) with \( ab = 0 \) satisfy (1.2); then \( y = 2 \) and \( a = 0, b = 1 \).

**Proof.** At first let \( a = 0 \). Then \( b \neq 0 \) because 3 is not a square. Further \( b = 1 \) leads to \( y^2 = 4 \) and so \( y = 2 \). If now \( b \geq 2 \) then \( 4 \mid 2^b \) and so

\[
y^2 \equiv 2 \pmod{4},
\]

impossible because \( y^2 \equiv 0, 1 \pmod{4} \).

Otherwise we have \( a \in \mathbb{N} \) and \( b = 0 \) which leads to

\[
y^2 \equiv 2 \pmod{3},
\]

impossible because \( y^2 \equiv 0, 1 \pmod{3} \). This completes the proof. \( \square \)

Therefore we may assume that \( a, b \) are in \( \mathbb{N} \).

**Lemma 3.2.** Let \( y, a, b \) in \( \mathbb{N} \) satisfy (1.2); then 6 divides \( y \).

**Proof.** We calculate (1.2) modulo 2. Then

\[
y^2 \equiv 3^a + 2^b + 1 \equiv 1 + 0 + 1 \equiv 0 \pmod{2},
\]

hence \( y^2 \) is even and so is \( y \).

Similarly we consider (1.2) modulo 3. Here

\[
(y + 1)(y - 1) \equiv y^2 - 1 \equiv 3^a + 2^b \equiv 2^b \not\equiv 0 \pmod{3}.
\]
So neither $y + 1$ nor $y - 1$ is divisible by 3 and hence 3 divides $y$, which completes the proof of the present lemma. □

Lemma 3.2 shows that $y = 6x$ for some $x$ in $\mathbb{N}$ and thus (1.2) appears as

\begin{equation}
36x^2 = 3^a + 2^b + 1.
\end{equation}

**Lemma 3.3.** Let $x, a, b$ in $\mathbb{N}$ satisfy (3.1). Then exactly one of the following holds:

1. $x = 1$ and either $a = 1, b = 5$ or $a = b = 3$,
2. $x$ is odd, $a \equiv 1 \pmod{8}$, and $b \equiv 3 \pmod{6}$ with $a \neq 1, b \neq 3$.

**Proof.** Considering (3.1) modulo 36 we get

\begin{equation}
0 \equiv 3^a + 2^b + 1 \pmod{36}.
\end{equation}

Further we calculate in the table below $3^n$ and $2^n$ modulo 36 for $1 \leq n \leq 8$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$3^n \pmod{36}$</th>
<th>$2^n \pmod{36}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$3^n$</td>
<td>3 9 27 9 27 9 27 9</td>
<td></td>
</tr>
<tr>
<td>$2^n$</td>
<td>2 4 8 16 32 28 20 4</td>
<td></td>
</tr>
</tbody>
</table>

Here we note that we get the same values for $n = 2$ and $n = 8$. Hence we see a period of length 6 when we calculate the table above for all $n$ in $\mathbb{N}$ or rather we get a partition of $\mathbb{N}$ with the classes

\begin{equation}
\{1\}_0 = \{1\}, \{2\}_6 = 2 + 6\mathbb{N}_0, \ldots, \{7\}_6 = 7 + 6\mathbb{N}_0.
\end{equation}

We now look for all $(a, b)$ with $1 \leq a, b \leq 7$ satisfying (3.2) and with the table above we find

$$(a, b) = (1, 5), (3, 3), (5, 3), (7, 3).$$

Together with (3.3) this implies that for $a, b \in \mathbb{N}$ we have either $a = 1$ and $b \in \{5\}_6$ or $a$ is in one of the sets $\{3\}_6, \{5\}_6, \{7\}_6$ and $b \in \{3\}_6$.

Consider first $a = 1$. Then (3.1) appears as

$$36x^2 = 2^b + 4$$

and hence

$$6x + 2)(6x - 2) = 2^b.$$

Thus $6x + 2$ and $6x - 2$ are powers of 2 and $(6x + 2) - (6x - 2) = 4$ yields $6x + 2 = 8$ and $6x - 2 = 4$ respectively; so $x = 1$ and $b = 5$.

Otherwise $a \neq 1$ is odd and $b \equiv 3 \pmod{6}$. Now $b = 3$ in (3.1) leads to

$$36x^2 = 3^a + 9$$

and similar to above we see that $6x + 3$ and $6x - 3$ are powers of 3 with $(6x + 3) - (6x - 3) = 6$; hence $x = 1$ and $a = 3$, which completes the first part of the lemma.
Let now \( b \neq 3 \). Since \( a \) is odd (3.1) yields
\[
36x^2 \equiv 3 + 0 + 1 \equiv 4 \pmod{8}
\]
and thus \( x \) is odd. So \( x = 2z + 1 \) and now
\[
36x^2 = 288\frac{z(z + 1)}{2} + 36 \equiv 4 \pmod{32}.
\]
Therefore (3.1) leads to
\[
3 \equiv 3^a \pmod{32}.
\]
For the values of \( 3^n \pmod{32} \) we consider the following table

\[
\begin{array}{c|ccccc}
 n & 1 & 3 & 5 & 7 & 9 \\
 3^n \pmod{32} & 3 & 27 & 19 & 11 & 3 \\
\end{array}
\]

Here we see a period of length 8 and hence that \( a \equiv 1 \pmod{8} \). Therefore the present lemma is proved. \( \square \)

**Lemma 3.4.** There are no \( x,a,b \) in \( \mathbb{N} \) with (3.1) which satisfy the conditions of the second part of Lemma 3.3.

**Proof.** Suppose that we have such \( x,a,b \) in \( \mathbb{N} \). We then consider (3.1) modulo 120. Therefore we use the table

\[
\begin{array}{c|ccc}
 n & 3 & 5 & 7 \\
 3^n \pmod{120} & 27 & 3 & 27 \\
 2^n \pmod{120} & 8 & 32 & 8 \\
\end{array}
\]

Similar to above we see a period of length 4 and \( a \equiv 1 \pmod{8} \) with \( a \neq 1 \) implies that \( a \) is in the set \( \{5\}_{12}, \{9\}_{12}, \{13\}_{12} \) and \( b \equiv 9 \pmod{12} \) shows

\[
36x^2 \equiv \begin{cases} 
36 \pmod{120}, & x \equiv \pm 1 \pmod{10}, \\
84 \pmod{120}, & x \equiv \pm 3 \pmod{10}, \\
60 \pmod{120}, & x \equiv 5 \pmod{10}.
\end{cases}
\]

Therefore we find that \( b \in \{5\}_4 \) as well because \( 36x^2 \not\equiv 12 \pmod{120} \). So the left side of (3.1) is \( 36 \pmod{120} \) and hence we have \( x \equiv \pm 1 \pmod{10} \). Further \( b \in \{5\}_4 \) implies that \( b \equiv 9 \pmod{12} \) because \( b \equiv 3 \pmod{6} \).

Next we consider (3.1) modulo 560. Therefore we use the following table

\[
\begin{array}{c|cccc}
 n & 5 & 9 & 13 & 17 \\
 3^n \pmod{560} & 243 & 83 & 3 & 243 \\
 2^n \pmod{560} & 32 & 512 & 352 & 32 \\
\end{array}
\]

Thus we see a period of length 12. Now \( a \equiv 1 \pmod{8} \) with \( a \neq 1 \) means that \( a \) is in one of the sets \( \{5\}_{12}, \{9\}_{12}, \{13\}_{12} \) and \( b \equiv 9 \pmod{12} \) shows
Further, $x \equiv \pm 1 \pmod{10}$ and we get
\[
36x^2 \equiv \begin{cases} 
36 \pmod{560}, & x \equiv \pm 1, \pm 29 \pmod{70}, \\
116 \pmod{560}, & x \equiv \pm 9, \pm 19 \pmod{70}, \\
436 \pmod{560}, & x \equiv \pm 11, \pm 31 \pmod{70}, \\
196 \pmod{560}, & x \equiv \pm 21 \pmod{70}; 
\end{cases}
\]
and thus we see that $a$ is not in the set $\{9\}_{12}$.

Finally, let us consider (3.1) modulo 208. Here we have a table
\[
\begin{array}{|c|c|c|c|c|}
\hline
n & 5 & 9 & 13 & 17 \\
\hline
3^n \pmod{208} & 35 & 131 & 3 & 35 \\
2^n \pmod{208} & 32 & 96 & 80 & 32 \\
\hline
\end{array}
\]
Again we see a period of length 12 and as above it follows that $a$ is in one of the sets $\{5\}_{12}, \{9\}_{12}, \{13\}_{12}$ and $b \in \{9\}_{12}$. And $x \in \mathbb{N}$ is odd so we find
\[
36x^2 \equiv \begin{cases} 
36 \pmod{208}, & x \equiv \pm 1 \pmod{26}, \\
116 \pmod{208}, & x \equiv \pm 3 \pmod{26}, \\
68 \pmod{208}, & x \equiv \pm 5 \pmod{26}, \\
100 \pmod{208}, & x \equiv \pm 7 \pmod{26}, \\
4 \pmod{208}, & x \equiv \pm 9 \pmod{26}, \\
196 \pmod{208}, & x \equiv \pm 11 \pmod{26}, \\
52 \pmod{208}, & x \equiv \pm 13 \pmod{26}. 
\end{cases}
\]
But this forces $a \in \{13\}_{12}$, which is a contradiction to above; and this completes the proof of the present lemma. \hfill \Box

Now the proof of Theorem 3.1 follows directly from the lemmas above.

References


Two exponential diophantine equations


Dominik J. Leitner
Mathematisches Institut
Universität Basel
Rheinsprung 21
4051 Basel, Switzerland
E-mail: dominik.leitner@unibas.ch