SKOLEM'S CONJECTURE CONFIRMED FOR A FAMILY OF EXPONENTIAL EQUATIONS, III

L. HAJDU, F. LUCA, AND R. TIJDEMAN

Dedicated to János Pintz on the occasion of his 70th birthday.

Abstract. We prove Skolem's conjecture for the exponential Diophantine equation $a^n + tb^n = \pm c^n$ under some assumptions on the integers a, b, c, t. In particular, our results together with Wiles' theorem imply that for fixed coprime integers a, b, c Fermat's equation $a^n + b^n = c^n$ has no integer solution $n \geq 3$ modulo m for some modulus $m := m(a, b, c)$ depending on a, b, c.

1. Introduction

Skolem's conjecture states that if a purely exponential Diophantine equation is not solvable, then it is not solvable modulo an appropriate modulus (see [12]). The conjecture and its variants have been proved only in certain special cases. One can mention results of Schinzel [9] concerning the one-term case, Bartolome, Bilu and Luca [1] concerning the case where the bases generate a multiplicative group of rank one, Hajdu and Tijdeman [7] concerning equations of the form $a^n - b^k = 1$, and Bérczes, Hajdu and Tijdeman [2] concerning equations of the form $a^n - tb_1^{k_1} \dots b_\ell^{k_\ell} = \pm 1$. See also Bertók and Hajdu [3, 4] for a result asserting that in some sense Skolem's conjecture is valid for "almost all" equations. For related problems and results concerning recurrence sequences, one can consult the papers [6, 8, 10, 11], and the references there and for a more detailed survey of the related literature, see [2] or [3].

Date: November 3, 2020.

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

Key words and phrases. Exponential Diophantine equations, Fermat's equation, Skolem's conjecture.

Research was supported in part by grants 115479, 128088 and 130909 of the Hungarian National Foundation for Scientific Research 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. F. L. worked on this paper during a 7 month research visit at the Max Planck Institute for Software Systems in Saarbrücken, Germany in late 2020 and early 2021.

In this note, we prove that under some natural assumptions, Skolem's conjecture is valid for the equations $a^n+tb^n = \pm c^n$. Note that our result contains the case of Fermat's equation $a^n + b^n = c^n$ with fixed coprime integers a, b, c.

2. The theorem

Theorem 2.1. *Let a, b, c, t be integers with $\gcd(a, b, c) = 1$ and $|b| \neq 1$, and let $\varepsilon \in \{-1, 1\}$. Then there exists a modulus m such that the congruence*

$$a^n + tb^n \equiv \varepsilon c^n \pmod{m} \tag{1}$$

has the same solutions in non-negative integers n as the equation

$$a^n + tb^n = \varepsilon c^n. \tag{2}$$

Further, such a modulus m can be effectively calculated in terms of a, b, c, t.

By the famous result of Wiles [14] on Fermat's Last Theorem for the case $|b| \neq 1$ and since the results in [2] imply that Skolem's conjecture holds for the equation $a^n - c^n = \pm 1$, the following statement follows from Theorem 2.1.

Corollary 2.1. *Let a, b, c be positive integers with $\gcd(a, b, c) = 1$. Then there exists a modulus m such that the congruence*

$$a^n + b^n \equiv c^n \pmod{m}$$

has no solutions in non-negative integers n with $n \geq 3$. Further, such a modulus m can be effectively calculated in terms of a, b, c.

We make some remarks.

Remarks. 1. We note that the coprimality condition in Theorem 2.1 cannot be dropped. Indeed, as one can easily check, the equations

$$0^n + 2^n = 4^n, \quad 2^n + 2^n = 4^n$$

have only the solutions $n = 0$ and $n = 0, 1$, respectively. However, they have infinitely many solutions modulo m for any m. This also means that the versions of Skolem's conjecture proposed in [3] and [4] should be carefully reformulated.

2. Observe that Corollary 2.1 implies the validity of Fermat's conjecture. However, this should not be interpreted as an elementary proof of Fermat's Last Theorem, as the proof of Corollary 2.1 via Theorem 2.1 relies on Wiles' theorem [14].

3. We note that there is a close connection between Theorem 2.1 with ternary linear recurrence sequences which we now describe. The

notation below will be used in our proof of Theorem 2.1. Let a, b, c, t be integers with $\gcd(a, b, c) = 1$ and $|b| > 1$, and let $\varepsilon \in \{\pm 1\}$. Consider the sequence $\mathbf{u} := \{u_n\}_{n\geq 0}$ given by

$$u_n := a^n + tb^n - \varepsilon c^n \qquad \text{for all} \quad n \geq 0. \tag{3}$$

This is a ternary recurrent sequence of integers, that is it satisfies a linear recurrence of order 3 with constant coefficients which we do not write down explicitly. Put

$$\mathcal{Z}_{\mathbf{u}} := \{n \geq 0 : u_n = 0\}.$$

The set $\mathcal{Z}_{\mathbf{u}}$ is called the zero set of the recurrence $\mathbf{u}$ and it is an object which has been frequently studied in the theory of linear recurrences. It follows from a famous theorem of Skolem–Mahler–Lech that $\mathcal{Z}_{\mathbf{u}}$ is finite. In our case the members of $\mathcal{Z}_{\mathbf{u}}$ are effectively computable using the theory of linear forms in p-adic logarithms. Indeed, let p be a prime factor of b. Write $\nu_p(m)$ for the exponent of p in the factorisation of m. Suppose that $\mathcal{Z}_{\mathbf{u}}$ contains a element $n_0 > 0$. If $p \mid ac$, then p divides both a and c, which is false. Thus, p does not divide ac and then

$$n_0 \leq \nu_p(tb^{n_0}) = \nu_p(a^{n_0} \pm c^{n_0}) \ll \log n_0.$$

The last inequality holds by linear forms in p-adic logarithms [13]. So, either there is a prime factor p of b which divides ac in which case $\mathcal{Z}_{\mathbf{u}} \subseteq \{0\}$, or p does not divide ac in which case the members of $\mathcal{Z}_{\mathbf{u}}$ are effectively computable.

3. An auxiliary result

In the proof of Theorem 2.1 we use the following lemma which nowadays is a simple consequence of a deep theorem of Bilu, Hanrot and Voutier [5]. However, the version below follows already from a classical result of Zsigmondy [15].

Lemma 3.1. *Let a, c be coprime non-zero integers with $|ac| > 1$. Then apart from at most four values of $n \geq 2$ the number $c^n - a^n$ has a primitive prime divisor, which is a prime factor p such that $p \nmid c^\ell - a^\ell$ for any $1 \leq \ell < n$. The same holds for $c^n + a^n$.*

Proof. The statement concerning $c^n - a^n$ immediately follows from Theorem C, Theorem 1.3 and Theorem 1.4 in [5]. The statement for $c^n + a^n$ is a direct consequence of this assertion as well upon noting that

$$c^n + a^n = \frac{c^{2n} - a^{2n}}{c^n - a^n} \qquad \text{holds for all} \qquad n \geq 1.$$

□

4. The proof of Theorem 2.1 in some special cases

In this section, we take care of some particular cases of Theorem 2.1.

We start with the case when $|a| = |c| = 1$. If $tb = 0$, then $m = 3$ is an appropriate modulus. If $tb \neq 0$, we then let p be a prime divisor of b and let q be an odd prime which does not divide tb. Then $m = p^2q(|tb| + 3)$ is an appropriate choice. Indeed, rewriting (1) as

$$tb^n \equiv \varepsilon c^n - a^n \pmod{m},$$

and considering it only modulo q first we see that $\varepsilon c^n - a^n \neq 0$. Then considering it modulo p^2, we obtain $n \leq 1$. Finally, considering it modulo $|tb| + 3$ we get that n is a solution of the congruence if and only if it is a solution to (2).

Next we prove Theorem 2.1 in the case where the numbers a, tb, c are not pairwise coprime.

If a and c are not coprime, then let p be a common prime factor of a and c. In view of the relation $\gcd(a, b, c) = 1$, we have $p \nmid b$. Thus, writing $r := \nu_p(t)$, the congruence

$$a^n + tb^n \equiv \varepsilon c^n \pmod{p^{r+1}}$$

gives $n \leq r$. Thus, taking $m = (|a|^r + |t||b|^r + |c|^r)p^{r+1}$, the theorem follows. Indeed, the congruence

$$a^n + tb^n - \varepsilon c^n \equiv 0 \pmod{m}$$

yields that $n \leq r$, so $|u_n| < m$ and $u_n \equiv 0 \pmod{m}$, which implies that $u_n = 0$.

Next assume that there is a prime factor p of tb such that $p \mid ac$. By what we have already shown, we may assume that p divides one of a, c but not both. We take $m = p(|t| + 3)$. Then the congruence

$$a^n + tb^n - \varepsilon c^n \equiv 0 \pmod{m}$$

implies that n cannot be positive otherwise p divides two of a^n, tb^n, c^n but not all three which is not possible. So, the only possibility is $n = 0$ which gives

$$1 + t - \varepsilon = u_0 \equiv 0 \pmod{|t| + 3}.$$

Since the integer on the left–hand side has absolute value less than the modulus, the congruence holds if and only if $u_0 = 0$. This proves the theorem also in this case.

Finally, consider the theorem in case $atbc = 0$. Since we may assume that $\gcd(a, c) = 1$ and $\gcd(tb, ac) = 1$, it follows that either $tb = 0$ and $|a| = |c| = 1$, or $|tb| = 1$, one of a, c is zero and the other is ± 1. One can easily see that the modulus $m = 3$ works in all these cases.

5. The proof of Theorem 2.1 in the general case

Throughout this proof p is prime factor of b. By the previous section, p is coprime to ac.

Consider first the case $\varepsilon = 1$. Let $z(p)$ the order of appearance of p in $\{a^n - c^n\}_{n\geq 0}$. This coincides with the order o_p of the residue class a/c modulo p, where $1/c$ modulo p stands for the inverse of c modulo p. It is also the smallest positive integer k such that $a^k - c^k \equiv 0 \pmod{p}$. Write $a^{z(p)} - c^{z(p)} = p^{\lambda_p} q$ for some integers $\lambda_p \geq 1$ and q coprime to p. Let $K = \omega(tb) + 6$, where $\omega(m)$ denotes the number of distinct prime factors of m.

Assume $n > \lambda_p + K$, $p^{\lambda_p+K} \mid m$ and $u_n \equiv 0 \pmod{p^{\lambda_p+K}})$. Then $p^{\lambda_p+K} \mid a^n - c^n$. By the properties of the order of appearance, we have that $z(p)p^{K-1} \mid n$. The numbers $a^{z(p)p^k} - c^{z(p)p^k}$ divide $a^n - c^n$ for $k = 0, \ldots, K-1$. Hence, by Lemma 3.1, for each $k \geq 0$ with at most 5 exceptions the number $a^{z(p)p^k} - c^{z(p)p^k}$ has a primitive divisor, namely a prime q_k, which does not divide $a^\ell - c^\ell$ for any $\ell < z(p)p^k$. Set $q_k = 1$ if k is an exception. Then $a^n - c^n$ is a multiple of $Q := q_0 \cdots q_{K-1}$. Now consider

$$m_1 := p^{\lambda_p+K} Q,$$

and look at the congruence $u_n \equiv 0 \pmod{m_1}$ when $n \geq n_1 := \lambda_p + K$. By the above argument, n is divisible by $z(p)p^{K-1}$, so $a^n - c^n$ is divisible by Q. Since the modulus is also divisible by Q, it follows that tb^n is divisible by Q. This is false, since $\omega(Q) \geq K - 5 > \omega(tb^n)$. Therefore, $n < n_1$.

Set

$$m := m_1 \prod_{\substack{0\leq s<n_1 \\ s\notin \mathcal{Z}_{\mathbf{u}}}} |u_s|. \tag{4}$$

We claim that m works. Indeed, m contains m_1 as a factor, so if $u_n \equiv 0 \pmod{m}$, then $n < n_1$. If $n \notin \mathcal{Z}_{\mathbf{u}}$, then

$$m_1 \cdot |u_n| \cdot \ell = m \mid u_n, \text{ where } \ell = \prod_{\substack{0\leq s<n_1 \\ s\neq n,\ s\notin \mathcal{Z}_{\mathbf{u}}}} |u_s|,$$

and $u_n \neq 0$. Thus, $m_1\ell = 1$, a contradiction in view of the fact that $m_1 > 1$.

Let now $\varepsilon = -1$. Then

$$u_n \equiv 0 \pmod{p}$$

yields that either $n = 0$ or

$$a^n + c^n \equiv 0 \pmod{p}. \tag{5}$$

The case $n = 0$ can be handled again using a modulus which is a multiple of $|t|+3$. So, we may focus on solutions $n > 0$ of (5). Assume that p is odd. Then a/c has even order o_p modulo p. Putting now $z(p) = o_p/2$, we have that

$$a^{z(p)} + c^{z(p)} \equiv 0 \pmod{p},$$

and $z(p)$ is the smallest positive integer s such that

$$a^s + c^s \equiv 0 \pmod{p}.$$

We take K similarly as in the case when $\varepsilon = 1$, namely $K = \omega(tb) + 6$. Consider the congruence $u_n \equiv 0 \pmod{p^{\lambda_p + K}}$, where we put again $\lambda_p := \nu_p(a^{z(p)} + c^{z(p)})$. As in the case $\varepsilon = 1$, we have $z(p)p^{K-1} \mid n$ and $n/(z(p)p^{K-1})$ is odd. The rest of the argument is similar to the case $\varepsilon = 1$. Namely, we work with $a^{z(p)p^\ell} + c^{z(p)p^\ell}$ where $\ell = 0, 1, \ldots, K-1$ which are all divisors of $a^n + b^n$ since p and $n/(z(p)p^{K-1})$ are both odd.

Assume now that b is a power of 2. Then a, c are odd. We now put $r := \nu_2(a + c)$. Then the congruence $u_n \equiv 0 \pmod{2^{r+1}}$ implies that $n \leq r$. Indeed, if $n \geq r+1$, we would then get that 2^{r+1} divides $a^n + c^n$. This is is not possible if n is even since then $\nu_2(a^n + c^n) = 1 < r+1$ and it is not possible if n is odd since $\nu_2(a^n + c^n) = \nu_2(a + c) = r < r + 1$. Hence, $n \leq r$. Now the proof finishes as in the case $\varepsilon = 1$ by taking m given by formula (4) with $m_1 = 2^{r+1}$ and n_1 replaced by $r + 1$.

Hence, the theorem follows also in this case, and the proof is complete.

□

6. Generalisations and an Open Problem

We start this section by reviewing the main idea of the proof of Theorem 2.1. It uses essential divisibility properties of the numbers $a^n - \varepsilon c^n$. In particular, our proof cannot be modified to cover values of the coefficient ε different from ± 1. The condition $|b| > 1$ guarantees that b has a prime factor p. Taking a modulus m divisible by p to a large exponent forces $a^n - \varepsilon c^n$ to be divisible by a large power of p which in turn forces n to be a multiple of $z(p)p^k$ for a large value of k. By the primitive divisor theorem Lemma 3.1, the number $a^{z(p)p^k} - \varepsilon c^{z(p)p^k}$ has many prime factors as k is large, namely the primitive prime factors of $a^{z(p)p^\ell} - \varepsilon c^{z(p)p^\ell}$ for $\ell = 0, 1, \ldots, k$. Taking a modulus m which incorporates these prime factors for $\ell = 0, 1, \ldots$, the congruence forces all these prime factors to also divide tb, which puts a bound on k. In a nut–shell that was the idea with the case $\varepsilon = -1$ and $p = 2$ requiring a bit of extra care. This simple idea can be generalised as follows:

Theorem 6.1. *Let $a, c, b_1, \dots, b_k, t$ be integers,* $\gcd(a, c, b_1 \dots b_k) = 1$, $|b_i| > 1$, *for $i = 1, \dots, k$. Let $\varepsilon = \pm 1$ and*

$$u(x, y_1, \dots, y_k) := a^x - \varepsilon c^x + t b_1^{y_1} \cdots b_k^{y_k}.$$

Put

$$\mathcal{Z}_{\mathbf{u}} = \{(x, y_1, \dots, y_k) \in \mathbb{Z}_{\geq 0}^{k+1} : x \leq \max\{y_i\},\ u(x, y_1, \dots, y_k) = 0\}.$$

Then $\mathcal{Z}_{\mathbf{u}}$ is finite. Furthermore, there exists $m := m(a, c, b_1, \dots, b_k, t)$ such that $u(x, y_1, \dots, y_k) \equiv 0 \pmod{m}$ implies $(x, y_1, \dots, y_k) \in \mathcal{Z}_{\mathbf{u}}$.

We only sketch the proof, which is based on the same idea. Namely, assume that y_1 is large. Take a prime factor p_1 of b_1 (assume p_1 is odd for simplicity) and incorporate a large power of p_1 into the modulus m. This forces $a^x - \varepsilon c^x$ to be divisible by a large power of p_1. It is possible that $a^x - \varepsilon c^x = 0$. This case can be taken care of by asking m to be divisible by a prime q not dividing $t b_1 \cdots b_k$. In the case when $a^x - \varepsilon c^x$ is not zero, the coprimality condition $\gcd(a, c, t b_1 \cdots b_k) = 1$ implies that ac is coprime to p_1 and that x is divisible by $z(p_1) p_1^{K_1}$ with a large K_1. Thus, $a^x - \varepsilon c^x$ is divisible by many "small primes", namely the primitive prime factors of $a^{z(p_1)p_1^\ell} - \varepsilon c^{z(p_1)p_1^\ell}$ for $\ell = 0, 1, \dots, K_1$. If K_1 is large and we incorporate all these primes into m, then the congruence implies that $t b_1 \dots b_k$ must be divisible by many primes which leads to a contradiction. This bounds y_1. The remaining exponents can be bounded in a similar way. The condition $x \leq \max\{y_1, \dots, y_k\}$ (or a more relaxed version of it asking x to be bounded in terms of $\max\{y_1, \dots, y_k\}$) is imposed in order to insure that once all the y_i's have been bounded, then x is bounded as well. The proof finishes by taking a modulus m which is also a multiple of the product of all the nonzero values of $u(x, y_1, \dots, y_k)$ in the bounded range of the nonzero integer variables $x, y_1, \dots, y_k$. It would be nice to obtain a similar conclusion without the condition x is bounded in terms of $\max\{y_1, \dots, y_k\}$. We leave this as a challenge to the reader.

Problem 6.1. *Does the conclusion of Theorem 6.1 hold without the hypothesis that x is bounded in terms of* $\max\{y_1, \dots, y_k\}$*?*

References

[1] B. Bartolome, Yu. Bilu and F. Luca, *On the exponential local-global principle*, Acta Arith. **159** (2013), 101–111.

[2] A. Bérczes, L. Hajdu and R. Tijdeman, *Skolem's conjecture confirmed for a family of exponential equations, II*, Acta Arith. (published online: 8 October 2020).

[3] Cs. Bertók and L. Hajdu, *A Hasse-type principle for exponential Diophantine equations and its applications*, Math. Comput. **85** (2016), 849–860.

[4] Cs. Bertók and L. Hajdu, *A Hasse-type principle for exponential Diophantine equations over number fields and its applications*, Monatsh. Math. **187** (2018), 425–436.
[5] Yu. Bilu, G. Hanrot, P.M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. reine angew. Math. 539 (2001), 75-122.
[6] K. A. Broughan and F. Luca, *On the Fürstenberg closure of a class of binary recurrences*, J. Number Theory **130** (2010), 696–706.
[7] L. Hajdu and R. Tijdeman, *Skolem's conjecture confirmed for a family of exponential equations*, will appear in Acta Arith.
[8] A. Ostafe and I. Shparlinski, *On the Skolem problem and some related questions for parametric families of linear recurrence sequences*, arXiv:2005.06713 [math.NT] 14 May 2020.
[9] A. Schinzel, *On power residues and exponential congruences*, Acta Arith. **27** (1975), 397–420.
[10] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), 245–274; Addendum and corrigendum, ibid. **36** (1980), 101–104.
[11] A. Schinzel, *On the congruence* $u_n \equiv c \pmod p$ *where* u_n *is a recurring sequence of the second order*, Acta Acad. Paedagog. Agriensis Sect. Math. **30** (2003), 147–165.
[12] Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, Avhdl. Norske Vid. Akad. Oslo I, 1937, no. 12, 16 pp.
[13] A. J. van der Poorten, *Linear forms in logarithms in the p-adic case*, in: Transcendence Theory; Advances and Applications, ed. by A. Baker and D.W. Masser, Academic Press, London etc., 1977, pp. 29-57.
[14] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. **141** (1995), 443–551.
[15] K. Zsigmondy, *Zur Theorie der Potenzreste*, J. Monatsh. Math. **3** (1892), 265–284.

L. Hajdu
Institute of Mathematics
University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: hajdul@science.unideb.hu

F. Luca
School of Mathematics
University of the Witwatersrand
Private Bag X3, WITS 2050
Johannesburg, South Africa
Research Group in Algebraic Structures and Applications
King Abdulaziz University, Jeddah, Saudi Arabia
E-mail address: Florian.Luca@wits.ac.za

R. Tijdeman
Mathematical Institute
Leiden University
Postbus 9512, 2300 RA Leiden, The Netherlands
E-mail address: tijdeman@math.leidenuniv.nl