SKOLEM'S CONJECTURE CONFIRMED FOR A FAMILY OF EXPONENTIAL EQUATIONS

L. HAJDU AND R. TIJDEMAN

Abstract. Skolem's conjecture states that if an exponential Diophantine equation is not solvable, then it is not solvable modulo an appropriately chosen modulus. Apart from many concrete equations, the conjecture has been proved only for rather special classes of equations. Here we show that the conjecture is valid for the Catalan equation $u^x - v^y = 1$ provided that one of u, v is a prime. This is the first instance where the conjecture is proved for a family of equations with more than one terms on the left hand side, of which the bases are multiplicatively independent.

1. Introduction

Skolem's conjecture [11] asserts that if an exponential Diophantine equation is not solvable, then it is not solvable modulo an appropriate modulus. This principle has been reformulated in slightly different forms in various papers; see e.g. Schinzel [7], Bartolome, Bilu and Luca [1] or Bertók and Hajdu [3, 4] for (closely related) variants. Note that some of these reformulations concern the rational case, others the algebraic one.

The conjecture and its variants have been proved only in very special cases. Schinzel [7] (extending results of Skolem [11]) proved the corresponding conjecture for equations of the form $\alpha_1^{x_1} \cdots \alpha_k^{x_k} = \beta$ where $\alpha_1, \ldots, \alpha_k$ and β are fixed elements of a number field, and $x_1, \ldots, x_k$ are unknown integers. Bartolome, Bilu and Luca [1] proved another appropriate version of the conjecture for equations of the shape $\lambda_1 \alpha_1^n + \cdots + \lambda_k \alpha_k^n = 0$, where $\lambda_1, \ldots, \lambda_k$, and $\alpha_1, \ldots, \alpha_k$ are elements of a number field K such that the multiplicative group generated by $\alpha_1, \ldots, \alpha_k$ is of order one, and n is a variable. We note that the results

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

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

Research was supported in part by grants K115479 and K128088 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.

in [1] can be derived from those in [7, 8] - though not in a straightforward way [10]. For other related results, see the papers [8, 9, 5] and the references therein. We mention that beside these, several particular equations have been treated by methods based upon Skolem's principle and its variants. Here we only mention the papers [3, 2, 4] and the references given there.

In the present paper we prove that Skolem's conjecture is valid for the Catalan equation $u^x - v^y = 1$, if u and v are fixed positive integers one of which is prime and x, y are non-negative integer variables. This equation has been studied thoroughly. By results of Mihăilesu [6] and several predecessors we know that the equation has no solutions with $\min(u, v, x, y) > 1$ apart from $(u, v, x, y) = (3, 2, 2, 3)$. Therefore to confirm Skolem's conjecture for this equation, it suffices to show that for every pair $(u, v) \neq (3, 2)$ there exists a modulus for which the corresponding congruence has no solution.

In fact, we shall give a more precise statement, under the extra condition that one of u, v is a prime. Our elementary method of proof will be the following. We establish certain properties $P_1, \dots, P_k$ concerning a putative solution modulo certain moduli $m_1, \dots, m_k$, respectively. If the system of these properties is contradicting (resp. allows only a finite number of solutions), then we get that the equation has no solutions (resp. has only the solutions obtained) modulo $m_1 \cdots m_k$ (in fact, already modulo $\mathrm{lcm}(m_1, \dots, m_k)$). Interestingly, at some points we can use a 'global-local' argument: the knowledge that some equation has no global solution is used to conclude that a certain congruence is not solvable.

2. The main result and its proof

Mihăilescu's celebrated result on Catalan's equation that we shall apply reads as follows.

Theorem 2.1 (Mihăilescu [6])**.** *Let u, v, x, y be integers all > 1. Then the only solution of the equation $u^x - v^y = 1$ is given by $u = 3$, $v = 2$, $x = 2$, $y = 3$.*

We shall derive the following extension towards Skolem's conjecture.

Theorem 2.2. *The equation $u^x - v^y = 1$ for fixed positive integers u, v with one of them prime has only the following solutions in nonnegative integer variables x, y:*
$x = 1$, $y = 0$, if $u = 2$ and v is any positive integer,
$x = 1$, y is arbitrary, if $(u, v) = (2, 1)$,
$x = a$, $y = 1$, if u is any prime and $v = u^a - 1$ for some $a \in \mathbb{Z}_{>0}$,

$x = 1$, $y = 2^b$, if u is a prime of the form $v^{2^b} + 1$ for some $b \in \mathbb{Z}_{>0}$,
$x = 1$, $y = a$, if v is any prime and $u = v^a + 1$ for some $a \in \mathbb{Z}_{>0}$,
$x = 2$, $y = 3$, if $(u, v) = (3, 2)$.
For every pair (u, v) with one of them prime there exists a modulus such that the corresponding congruence has no other solutions than the Diophantine equation itself has.

Remark 1. It will be clear from the proof that given u, v, the modulus m can be explicitly constructed, and can be bounded in terms of u and v.

Remark 2. Theorem 2.2 and its proof can be reformulated for a related class of equations, having no solutions at all. For example, we have that there exists a modulus m such the congruence

$$u^2 \cdot u^x - v^2 \cdot v^y \equiv 1 \pmod{m} \quad ((u, v) \neq (3, 2) \text{ and one of } u, v \text{ is a prime})$$

has no solutions in non-negative integers x, y.

Proof of Theorem 2.2. We shall consider the equation

$$u^x - v^y = 1 \tag{1}$$

modulo different moduli where x, y are nonnegative integers. The proof is split in cases $(u, v) = (3, 2)$, $u = 2$, u is an odd prime, and v is prime.

First we consider $(u, v) = (3, 2)$. We investigate equation (1) modulo 16, 27 and 73. Modulo 16 equation (1) yields that we are in one of the cases

- $x \equiv 1 \pmod 4$ and $y = 1$,
- $x \equiv 2 \pmod 4$ and $y = 3$,
- $4 \mid x$.

From (1) modulo 27 we get that one of the following holds:

- $x = 1$ and $y \equiv 1 \pmod{18}$,
- $x = 2$ and $y \equiv 3 \pmod{18}$,
- $9 \mid y$.

Finally, modulo 73 equation (1) yields that we have one of

- $x \equiv 1 \pmod{12}$ and $y \equiv 1 \pmod 9$,
- $x \equiv 2 \pmod{12}$ and $y \equiv 3 \pmod 9$,
- $x \equiv 10 \pmod{12}$ and $y \equiv 6 \pmod 9$.

Hence, in this case the only solutions of (1) mod $16 \cdot 27 \cdot 73$ are given by $(x, y) = (1, 1)$ and $(2, 3)$.

In what follows, without further mentioning we use that modulo $v+1$ we get that

$$x \neq 0. \tag{2}$$

Now we consider the case $u = 2$. We start with the subcase $u = 2$, v is even. Then equation (1) modulo 4 gives either $x = 0$, or $x = 1$, $y = 0$. Hence we see that for $u = 2$, v is even the congruence

$$2^x - v^y \equiv 1 \pmod{4(v+1)}$$

has only the solution $(x, y) = (1, 0)$.

Subsequently we consider the subcase $u = 2$, $v = 1$. Then equation (1) modulo 4 implies $x = 1$ and y is arbitrary.

Next consider the subcase $u = 2$, $v > 1$, v is odd. First we handle solutions (x, y) with y even. For such solutions equation (1) yields

$$2^x \equiv 2 \pmod{v-1}, \quad 2^x \equiv 2 \pmod{v+1}. \tag{3}$$

As v is odd, we have $4 \mid v-1$ or $4 \mid v+1$. Thus congruences (3) can hold simultaneously only if $x = 1$. Further, (1) modulo v gives that

$$\text{if } x = 1 \text{ then } y = 0. \tag{4}$$

Thus in this subcase the only solution with y even of (1) modulo $v(v+1)(v-1)$ is $(x, y) = (1, 0)$.

If y is odd, then equation (1) yields

$$2^x \equiv 2 \pmod{v-1}, \quad 2^x \equiv 0 \pmod{v+1}. \tag{5}$$

The second congruence gives that $v + 1 \mid 2^x$, hence v must be of the form $v = 2^a - 1$ with some fixed $a \geq 2$. Thus we can write equation (1) as

$$2^x - (2^a - 1)^y = 1 \quad (a \geq 2), \tag{6}$$

where modulo 2^a we get $x \geq a$. If $x > a$, then (6) modulo 2^{a+1}, in view of that y is odd, gives a contradiction. If $x = a$, then (6) modulo $(2^a-1)^2$ yields $y = 1$. So modulo $2^{a+1}(2^a-1)^2$ we get that $(x, y) = (a, 1)$ in this case.

Summarizing, in the subcase $u = 2$, $v > 1$, v is odd we have that the only solutions of equation (1) modulo $2(v+1)(v-1)v^2$ are given by $(x, y) = (1, 0), (a, 1)$. In the latter case v is of the form $v = 2^a - 1$. This concludes our treatment of the case $u = 2$.

Assume now that u is an odd prime. We write $u - 1 = 2^k u_0$ with u_0 odd. Then if $x > 0$ the congruence

$$v^y \equiv -1 \pmod{u},$$

obtained from (1), implies that the exponent of 2 in y is at most $k-1$. Write $y = 2^b z$ with z odd and $0 \le b \le k-1$. Then equation (1) can be rewritten as

$$u^x - \left(v^{2^b}\right)^z = 1. \tag{7}$$

This equation modulo $v^{2^b}+1$ yields $v^{2^b}+1 \mid u^x$. So we have $v^{2^b}+1 = u^a$ with some bounded $a \ge 1$. However, by Theorem 2.1 we know that this may happen only when $a = 1$ or $b = 0$. That is, either $v^{2^b}+1 = u$ for some b with $1 \le b \le k-1$, or (1) modulo $\prod_{b=0}^{k-1}(v^{2^b}+1)$ implies that y is odd.

So if u is an odd prime then solutions (x, y) with y even may only occur if $u = v^{2^b}+1$ for some b with $1 \le b \le k-1$ and (1) can be rewritten as

$$(v^{2^b}+1)^x - (v^{2^b})^z = 1, \tag{8}$$

where z is odd. We know that $v > 1$, because u is odd. If $z \ge 3$, then (8) modulo $v^{2^{b+1}}$ yields $v \mid x$. Furthermore (8) modulo $(v^{2^b}+1)^v - 1$ implies

$$(v^{2^b}+1)^v - 1 \mid v^{2^b z}.$$

By expanding the left-hand side we get $v^{2^b+1}(tv+1) \mid v^{3\cdot 2^b}$ for some integer $t > 0$ using that $b > 0$. This is impossible. If $z = 1$, then from (8) modulo $(v^{2^b}+1)^2$ we get that $x = 1$. Summarizing, in this subcase the only solution of equation (1) modulo $v^{2^b+1}((v^{2^b}+1)^v - 1)(v^{2^b}+1)^2$ is $(x, y) = (1, 2^b)$ provided that $u = v^{2^b}+1$ is an odd prime.

Still supposing that u is an odd prime, now we look at the solutions (x, y) with y is odd. We consider (1) modulo $v+1$ and obtain $v+1 \mid u^x$. Then v is of the form $v = u^d - 1$ with some fixed $d \ge 1$, and we can rewrite (1) as

$$u^x - (u^d - 1)^y = 1.$$

The above equation modulo u^d yields that $x \ge d$. If $x = d$, then (1) modulo $(u^d-1)^2$ immediately yields $y = 1$. If $x > d$, then modulo u^{d+1} we would get $u \mid y$. Then modulo $(u^d-1)^u+1$ we get $(u^d-1)^u+1 \mid u^x$, whence $(u^d-1)^u + 1 = u^e$ with $e > 0$ fixed. By Theorem 2.1 this implies $(u, v) = (3, 2)$, which has been considered already. Altogether we see that the only solution of (1) modulo $u^{d+1}((u^d-1)^u+1)(u^d-1)^2$ in this subcase excluding $(u, v) = (3, 2)$ is given by $(x, y) = (d, 1)$ when $v = u^d - 1$.

We can summarize the case where u is an odd prime and $(u, v) \ne (3, 2)$ as follows:

- if $u = v^{2^b} + 1$ for some b with $1 \leq b \leq k-1$ then equation (1) modulo $v(u-1)(u^v-1)u^2$ has the only solution $(x, y) = (1, 2^b)$,
- if $v = u^d - 1$ with some $d \geq 1$ then (1) modulo $u(v+1)(v^u+1)v^2$ has the only solution $(x, y) = (d, 1)$,
- if none of the above relations hold for u, v then equation (1) has no solutions modulo $\prod_{b=0}^{k-1}(v^{2^b} + 1)$.

Consider now the case v is a prime. We immediately see modulo v that $u \neq 1$. Further, by what we have proved already, we may also assume that $u > 2$. Taking (1) modulo $u-1$ we find that $u-1$ has to be of the form $u - 1 = v^a$ with some fixed $a \geq 1$. Hence equation (1) takes the form

$$(v^a + 1)^x - v^y = 1 \quad (a \geq 1). \tag{9}$$

This equation modulo v^a shows that $y \geq a$. If $y = a$, then modulo $(v^a + 1)^2$ we get that $x = 1$. If $y > a$, then considering equation (9) modulo v^{a+1}, we get that $v \mid x$. Then modulo $(v^a + 1)^v - 1$ we obtain that $(v^a + 1)^v - 1 \mid v^y$. So $(v^a + 1)^v - 1 = v^b$ with some fixed $b \geq 1$. In view of Theorem 2.1 this implies $(u, v) = (3, 2)$, which has been considered already. Summarizing, we get that in this case excluding $(u, v) = (3, 2)$, the only solution of (1) modulo $u^2v(u-1)(u^v-1)(v+1)$ is given by $(x, y) = (1, a)$ in case $u - 1$ is of the form v^a.

On combining all the above results we conclude that Theorem 2.2 is valid. □

References

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

[2] Cs. Bertók, *The complete solution of the Diophantine equation* $(4m^2 + 1)^x + (5m^2 - 1)^y = (3m)^z$, Period. Math. Hung. **72** (2016), 37–42.

[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] K. A. Broughan and F. Luca, *On the Fürstenberg closure of a class of binary recurrences*, J. Number Theory **130** (2010), 696–706.

[6] P. Mihăilescu, *Primary Cyclotomic Units and a Proof of Catalan's Conjecture*, J. Reine angew. Math. **572** (2004), 167–195.

[7] A. Schinzel, *On power residues and exponential congruences*, Acta Arith. **27** (1975), 397–420.

[8] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), 245–274; Addendum and corrigendum, ibid. **36** (1980), 101–104.

[9] 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.
[10] A. Schinzel, *Private communication.*
[11] Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, Avhdl. Norske Vid. Akad. Oslo I, 1937, no. 12, 16 pp.

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

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