The proof of Skolem's conjecture for certain three term equations

L. Hajdu

University of Debrecen

Specialisation and Effectiveness in Number Theory

Banff International Research Station

28 August - 2 September, 2022

Plan of the talk

- A (very) brief history of Skolem's conjecture

- The proof of Skolem's conjecture for equations $x^n - by_1^{k_1} \cdots y_\ell^{k_\ell} = \pm 1$

- The proof of Skolem's conjecture for equations $x^n + by^n = \pm z^n$

The new results are joint with **A. Bérczes, F. Luca, R. Tijdeman**.

Skolem's conjecture

Skolem's conjecture: if an exponential Diophantine equation is not solvable, then it is not solvable modulo m for some m

Schinzel (1975): The conjecture is true for equations

$$b_1^{\alpha_1} \cdots b_\ell^{\alpha_\ell} = c.$$

Bartolome, Bilu and Luca (2013): The conjecture is true for equations of the form

$$a_1 b_1^{\alpha_1} + \cdots + a_\ell b_\ell^{\alpha_\ell} = 0,$$

if the rank of the multiplicative group generated by $b_1, \ldots, b_\ell$ is one.

These results also hold over number fields.

New results

Theorem 1 (Bérczes, H, Tijdeman)

Let $b, x, y_1, \dots, y_\ell$ be given integers. Then there exists a modulus m such that the congruence

$$x^n - by_1^{k_1} \cdots y_\ell^{k_\ell} \equiv \pm 1 \pmod{m} \tag{1}$$

has precisely the same solutions in non-negative integers $n, k_1, \dots, k_\ell$ as the equation

$$x^n - by_1^{k_1} \cdots y_\ell^{k_\ell} = \pm 1 \tag{2}$$

has.

This result extends an earlier theorem of **H and Tijdeman**, concerning (2) with $b = \ell = 1$ and one of x, y being a prime.

Some remarks

Remark 1

It will be clear from the proof that given $b, x, y_1, \ldots, y_\ell$*, the modulus* m *can be explicitly constructed, and can be bounded in terms of* $b, x, y_1, \ldots, y_\ell$*.*

Remark 2

Theorem 1 covers the famous equations $x^n - y^k = 1$ *and* $\frac{x^n-1}{x-1} = y^k$ *for fixed* x, y*.*

Remark 3

Theorem 1 can be reformulated for a related class of equations, having no solutions at all. E.g., there is an m *such the congruence*

$$x^n - y^k \equiv 1 \pmod{m} \quad (x, y \textit{ fixed},\ (x, y) \neq (3, 2))$$

has no solutions in integers $n > 1$, $k > 1$*.*

Strategy of the proof

Recall the congruence and the equation

$$x^n - by_1^{k_1} \cdots y_\ell^{k_\ell} \equiv \pm 1 \pmod{m} \tag{1}$$

$$x^n - by_1^{k_1} \cdots y_\ell^{k_\ell} = \pm 1 \tag{2}$$

For every m all solutions of (2) are solutions of (1).

So it suffices to prove that for certain m every solution of (1) is a solution of (2).

For fixed $b, x, y_1, \dots, y_\ell$, write S_∞ for the set of solutions of (2) and for any modulus m let S_m be the set of solutions of (1).

Then $S_\infty \subseteq S_m$ for any $m \geq 2$.

Strategy of the proof - continued

On the other hand, if $m_1, m_2 \mid m$ then $S_m \subseteq S_{m_1} \cap S_{m_2}$. So if

$$\bigcap_{i=1}^{t} S_{m_i} = S_\infty$$

then the following choice is appropriate:

$$m := \prod_{i=1}^{t} m_i.$$

If the terms of all the solutions of (1) are bounded modulo m', then we may choose m'' sufficiently large so that modulo $m = m'm''$, (1) and (2) have exactly the same solutions.

Strategy of the proof - continued

Let S be a finite set of primes, and write U_S for the set of integers having all their prime divisors in S.

The following theorem will play an important role later on.

Theorem A

The equation $v_1 - v_2 = c$ where c is a non-zero integer has only finitely many solutions in $v_1, v_2 \in U_S$, whose number can be effectively bounded in terms of S, c. (See results of **Evertse, Győry** *and others.)*

Proof sketch for $x^n - by^k = 1$

We focus on the case $\ell = 1$ and $+1$ on the RHS:

$$x^n - by^k = 1. \tag{3}$$

The case -1 on the RHS is more involved but similar, and $\ell > 1$ can be handled inductively.

If $|x| \leq 1$, $|y| \leq 1$ or $\gcd(x, by) > 1$ then the situation is simple.

Consider $x^n - by^k = 1$ for fixed b, x, y. It is an S-unit equation.

Write N for the number of solutions.

Proof sketch for $x^n - by^k = 1$

Let s_1 be the smallest integer such that

$$|y|^{s_1} > |x| + 1.$$

Observe that s_1 can be easily expressed in terms of x, y.

If $k < s_1$, then k is bounded and can be considered to be fixed. So we may suppose $k \geq s_1$.

Then we get

$$x^n \equiv 1 \pmod{|y|^{s_1}}.$$

Proof sketch for $x^n - by^k = 1$

Thus the order o_1 of x modulo $|y|^{s_1}$ must divide n.

This order is not one, so

$$2 \leq o_1 \leq |y|^{s_1}.$$

Let now s_2 be the smallest integer such that

$$|y|^{s_2} > |x|^{o_1} + 1.$$

Observe that o_1 and s_2 are bounded in terms of x, y.

If $k < s_2$ we can proceed as in the case $k < s_1$. So we may assume that $k \geq s_2$.

Proof sketch for $x^n - by^k = 1$

Hence we obtain

$$x^n \equiv 1 \pmod{|y|^{s_2}}.$$

Therefore the order o_2 of x modulo $|y|^{s_2}$ must also divide n.

We have $o_1 \mid o_2$, too.

Further, by our choice of s_2 we see that

$$1 < o_1 < o_2 \le |y|^{s_2}.$$

Proof sketch for $x^n - by^k = 1$

Continuing this procedure, we have two options.

Either the process terminates in at most N steps, yielding modulo $|y|^{s_i}$ for some $i \leq N$ that k is bounded in terms of b, x, y.

Then we are done.

Or, after N steps we obtain that there exist divisors $o_1, \dots, o_N$ of n with

$$1 < o_1 < \cdots < o_N \leq |y|^{s_N}$$

where s_N is bounded in terms of x, y, such that

$$o_1 \mid o_2, \dots, o_{N-1} \mid o_N, o_N \mid n.$$

Proof sketch for $x^n - by^k = 1$

Put $o_0 = 1$ and consider (3) modulo $x^{o_i} - 1$ for $i = 0, 1, \ldots, N$.

We get that for $k \geq s_N$

$$by^k \equiv 0 \pmod{x^{o_i} - 1}$$

holds, hence $x^{o_i} - 1 \in U_S$ ($i = 0, 1, \ldots, N$).

However, then there are $N + 1$ solutions, contradicting the definition of N. (Note that it is a funny 'global-local principle'.)

So taking the modulus

$$m' = |y|^{s_N}$$

we get that in all solutions of $x^n - by^k = 1$ modulo m', we have $k < s_N$.

From this, as we already mentioned, our claim follows.

New results

Theorem 2 (H, Luca, Tijdeman)

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

$$x^n + by^n \equiv \varepsilon z^n \pmod{m}$$

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

$$x^n + by^n = \varepsilon z^n.$$

Further, such a modulus m can be effectively calculated in terms of x, y, z, b.

Remark 4

In fact we obtained a more general, but also more technical result.

Proof sketch for $x^n + by^n = z^n$

We restrict to the equation $x^n + by^n = z^n$ (i.e, $\varepsilon = 1$), the case $\varepsilon = -1$ is similar.

The cases where $|x| = |z| = 1$, $bxyz = 0$ or when x, by, z are not pairwise coprime can be handled easily.

Also, if we can find a modulus M such that the solutions n to $x^n + by^n \equiv z^n \pmod{M}$ are bounded, we are easily done.

A proof similar to that of Theorem 1 would work.

However, now a simpler argument is available, related to recurrence sequences and primitive divisors.

Proof sketch for $x^n + by^n = z^n$

Let $p \mid y$; then $p \nmid xz$.

Let $o(p)$ be the order of appearance of p in $\{x^n - z^n\}_{n \geq 0}$.

Write $x^{o(p)} - z^{o(p)} = p^{\lambda_p} q$ for some integers $\lambda_p \geq 1$ and q coprime to p.

Let $K = \omega(by) + 6$, where $\omega(N)$ denotes the number of distinct prime factors of N.

Let $p^{\lambda_p + K} \mid m$, and assume that $x^n + by^n \equiv z^n \pmod{m}$. If n is a solution with $n \geq \lambda_p + K$ then $p^{\lambda_p + K} \mid x^n - z^n$.

By the properties of $o(p)$ we have $o(p)p^{K-1} \mid n$. Thus $x^{o(p)p^k} - z^{o(p)p^k}$ divides $x^n - z^n$ for $k = 0, \ldots, K-1$.

Proof sketch for $x^n + by^n = z^n$

By a classical result of Zsigmondy, for each $k \geq 0$ with at most 5 exceptions the number $x^{o(p)p^k} - z^{o(p)p^k}$ has a primitive prime divisor q_k.

Set $q_k = 1$ if k is an exception. Then $x^n - z^n$ is a multiple of $Q := q_0 \cdots q_{K-1}$.

Look at the congruence $x^n + by^n \equiv z^n \pmod{p^{\lambda_p + K} Q}$.

If n is a solution with $n \geq \lambda_p + K$, then n is divisible by $o(p)p^{K-1}$, so $x^n - z^n$ is divisible by Q.

Thus by^n is divisible by Q. This is false, since $\omega(Q) \geq K - 5 > \omega(by^n)$. Therefore $n < \lambda_p + K$.

Two interesting corollaries

Corollary 1

Let x, y be positive integers. Then there exists a modulus m such that

$$x^k - y^\ell \equiv 1 \pmod{m}$$

has no solutions in integers k, ℓ with $k, \ell \geq 2$, $(k, \ell) \neq (2, 3)$ for $(x, y) = (3, 2)$. Further, such a modulus m can be effectively calculated in terms of x, y.

Corollary 2

Let x, y, z be coprime positive integers. Then there exists a modulus m such that

$$x^n + y^n \equiv z^n \pmod{m}$$

has no solution in integer n with $n \geq 3$. Further, such a modulus m can be effectively calculated in terms of x, y, z.

The mentioned papers related to Skolem's conjecture

- B. Bartolome, Yu. Bilu and F. Luca, *On the exponential local-global principle*, Acta Arith. **159** (2013), 101-111.
- A. Bérczes, L. Hajdu and R. Tijdeman, *Skolem's conjecture confirmed for a family of exponential equations, II*, Acta Arith. 197 (2021), 129-136.
- L. Hajdu, F. Luca and R. Tijdeman, Skolem's conjecture confirmed for a family of exponential equations III, J. Number Theory 224 (2021), 41–49.
- L. Hajdu and R. Tijdeman, *Skolem's conjecture confirmed for a family of exponential equations*, Acta Arith. 192 (2020), 105-110.
- A. Schinzel, *On power residues and exponential congruences*, Acta Arith. **27** (1975), 397-420.
- Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, Avhdl. Norske Vid. Akad. Oslo I, 1937, no. 12, 16 pp.