On equation $X^n - B.Y^n = 1$

Boris Bartolomé

Göttingen Universität & Institut de Mathémathiques de Bordeaux

Boris.Bartolome@mathematik.uni-goettingen.de

Boris.Bartolome@math.u-bordeaux1.fr

January 25th, 2016

Overview

Binary Thue: prologue

This is a joint work with Preda Mihăilescu. We call binomial Thue equation:

$$A.X^n - B.Y^n = C,$$

where $n \geq 3$ and A, B and C are non-zero integers. Thue proved in 1909 that, for a fixed n, this equation has at most a finite number of solutions in integers (x, y). Currently, even the best numerical bounds on the solutions are too large for numerical resolution. This equation has been totally solved in some particular cases, always with $C = \pm 1$. We study equation:

$$X^n - B.Y^n = 1, \tag{1}$$

which we call Binary Thue.

Binary Thue: prologue

Previous results:

- Michael Bennett [Be] proves that when $C = \pm 1$ in equation $A.X^n - B.Y^n = C$, there is at most one solution for fixed $(A, B; n)$,
- Bassó + Bérczes + Györy + Pintér [BBGP] prove that Binary Thue has no solutions for $B < 235$.
- Buhler and Harvey recently proved [BH] that condition CF is verified for primes up to 163.10^6.

We prove that there are no solutions for families of density one of numbers B and n, and we show the form of the potential solution in the other cases.

Binary Thue: prologue

Let $B \in \mathbb{Z}, n \in \mathbb{N}_{>1}$, define $\varphi^*(B) := \varphi(\mathrm{rad}\ (B))$, where $\mathrm{rad}\ (B)$ is the radical of B, and assume that:

$$(n, \varphi^*(B)) = 1.$$

More generally, for a fixed $B \in \mathbb{Z}$ we let

$$\mathcal{N}(B) = \{n \in \mathbb{N}_{>1} \mid \exists\ k > 0 \text{ such that } n | \varphi^*(B)^k\}.$$

If p is an odd prime, we shall denote by CF the combined condition requiring that

I The Vandiver Conjecture holds for p, so the class number h_p^+ of the maximal real subfield of the cyclotomic field $\mathbb{Q}[\zeta_p]$ is not divisible by p.

II The index of irregularity of p is small, namely $i_r(p) < \sqrt{p} - 1$, so there are $i_r(p)$ odd integers $k < p$ such that the Bernoulli number $B_k \equiv 0 \bmod p$.

Binary Thue

Theorem (Bartolomé, Mihăilescu, 2015)

Let n be a prime and $B > 1$ an integer with $(\varphi^*(B), n) = 1$. Suppose that BT has a non trivial integer solution different from $n = 3$ and $(X, Z; B) = (18, 7; 17)$. Let $X \equiv u \bmod n$, $0 \leq u < n$ and $e = 1$ if $u = 1$ and $e = 0$ otherwise. Then:

1. $n > 163 \cdot 10^6$.
2. $X - 1 = \pm B/n^e$ *and* $B < n^n$.
3. *If* $u \notin \{0, 1, n-1\}$, *then condition CF (II) fails for* n *and*

$$\begin{aligned} 2^{n-1} &\equiv 3^{n-1} \equiv 1 \mod n^2, \quad \text{and} \\ r^{n-1} &\equiv 1 \mod n^2 \quad \text{for all } r | X(X^2-1). \end{aligned}$$

If $u \in \{0, 1, n-1\}$, *then Condition CF (I) fails for* n.

Binary Thue

Theorem (Bartolomé, Mihăilescu, 2015)

If Equation $X^n - 1 = B.Z^n$ has a solution for a fixed B verifying $(n, \varphi^*(B)) = 1$, then either $n \in \mathcal{N}(B)$ or there is a prime p coprime to $\varphi^*(B)$ and an $m \in \mathcal{N}(B)$ such that $n = p \cdot m$. Moreover X^m, Z^m is a solution of $X^p - 1 = B.Z^p$ for the prime exponent p and thus verifies the conditions of the previous theorem.

From diagonal Nagell – Ljunggren to binary Thue

Any solution of diagonal Nagell – Ljunggren leads to a solution of binary Thue.

We remind that diagonal Nagell – Ljunggren is:

$$\frac{X^n-1}{X-1} = n^e Y^n, \quad e = \begin{cases} 0 & \text{if } X \not\equiv 1 \bmod n, \\ 1 & \text{otherwise.} \end{cases} \tag{2}$$

Let (X, Y) be a solution of diagonal Nagell – Ljunggren. Then $(X, Y; n^e(X-1))$ is a solution of binary Thue. For instance, the particular solution $(X, Y; B) = (18, 7; 17)$ of binary Thue stems from

$$\frac{18^3-1}{18-1} = 7^3,$$

which is supposed to be the only non trivial solution of diagonal Nagell – Ljunggren.

From binary Thue to diagonal Nagell – Ljunggren

Any solution of $X^n - 1 = B \cdot Z^n$ leads to a solution of diagonal Nagell – Ljunggren.

We prove that any prime $p_i \in \mathbb{Z}$, in the radical of $\frac{X^n-1}{n^e(X-1)}$, is coprime with all of its conjugates in $\mathbb{Z}[\zeta]$, and they are thus totally split. Such p_i are also in the radical of $X^n - 1$. Therefore, if (X, Z) is a solution of binary Thue, then there exists $C \in \mathbb{Z}$ such that $Z = C \cdot Y$ and

$$\frac{X^n - 1}{n^e(X-1)} = Y^n \quad \text{and} \tag{3}$$

$$X - 1 = B \cdot C^n / n^e. \tag{4}$$

Bounds to the solutions of diagonal Nagell – Ljunggren

Theorem (Theorem 3 from [Mi])

Suppose that X, Y are integers solutions of diagonal Nagell – Ljunggren, with $n \geq 17$ being a prime. Let $u = (X \bmod n)$. Then there is an $E \in \mathbb{R}_+$ such that $|X| < E$. The values of E in the various cases of the equation are the following:

$$E = \begin{cases} 4 \cdot \left(\frac{n-3}{2}\right)^{\frac{n+2}{2}} & \text{if } u \notin \{-1, 0, 1\} \\ (4n)^{\frac{n-1}{2}} & \text{if } u = 0\ , \\ 4 \cdot (n-2)^n & \text{otherwise.} \end{cases}$$

Sketch of the proof of the main Theorem

1. Claims (1) and (3) come directly from [Mi], by applying the link between binary Thue and diagonal Nagell – Ljunggren.
2. We have already proved that $X - 1 = B \cdot C^n / n^e$. If $C = \pm 1$, then $X - 1 = \pm B / n^e$, as stated in point (2) of the Theorem and X is a solution of diagonal Nagell – Ljunggren. The bounds on $|X|$ in Theorem 3 from [Mi] imply $|B| < n^n$, the second claim of (2).
3. The rest of the presentation consists is proving that $C = \pm 1$. It is quite technical.

Sketch of the proof that $C = \pm 1$: notation

Assume that (X, Z, B) verifies Binary Thue. Let $\alpha = \frac{X-\zeta}{(1-\zeta)^e} \in \mathbb{Z}[\zeta]$, $\mathbb{K} = \mathbb{Q}(\zeta)$. According to (3), $\mathbf{N}_{\mathbb{K}/\mathbb{Q}}(\alpha) = Y^n$ (where $Z = C.Y$). Let $\sigma_c \in G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) : \zeta \to \zeta^c$, I be the Stickelberger ideal of $\mathbb{Z}[G]$. The *absolute weight* of $\sum_c n_c\sigma_c \in \mathbb{Z}[G]$ is $\sum_c |n_c|$. The Fermat quotient map $I \to \mathbb{Z}/(n.\mathbb{Z})$ given by

$$\varphi : \theta = \sum_{c=1}^{n-1} n_c\sigma_c \to \sum_{c=1}^{n-1} cn_c \mod n$$

has kernel $I_f = \{\theta \in I : \zeta^\theta = 1\}$. Let $I_f^+ \subset I_f$ the subset of positive elements of I_f (that is, elements $\sum_c n_c\sigma_c \in I_f$ such that for all c, $n_c \geq 0$) Let $\sum_c n_c = \varsigma(\theta).\frac{n-1}{2}$, where $\varsigma(\theta)$ is the *relative weight* of θ. Finally, let p be a prime dividing C (then, by (4), p also divides $X - 1$).

Galois exponent

Suppose we know that $(1+x)$ is β^q for some $\beta \in \mathbb{Q}(\zeta_p)$. Then, $\beta = \xi_q^\kappa f(x)$ where $f(x)$ is the sum of the binomial series. κ is unknown.

When we act on $(1+x)$ with an element $\theta \in \mathbb{F}_q[G]$, the sum of the binomial series $f(\theta x) = (1+x)^{\theta/q}$ differs from β^θ by a q-th root of unity depending on θ. We denote the exponent of this q-th root of unity, the Galois exponent, $\kappa(\theta)$, so we have

$$\beta^\theta = \xi_q^{\kappa(\theta) f(\theta x)}$$

Lemma

For any $\theta \in 2.I_f^+$, for any prime ideal $\mathfrak{P} \mid p$, there is a $\kappa = \kappa_{\mathfrak{P}}(\theta) \in \mathbb{Z}/(n \cdot \mathbb{Z})$ such that

$$\beta[\theta] \equiv \zeta^{\kappa} \cdot Y^{\frac{\varsigma(\theta)}{2}} \bmod \mathfrak{P}. \tag{5}$$

We prove that the decomposition group of p contains at least three distinct elements. This allows us to build $\mu \in \mathbb{F}_p[G]$ small enough (of small *absolute weight* $h/2$), such that $\kappa = 0$. Using this μ, we then build $\Theta \in 2.I_f^+$ with also $\kappa = 0$ and some additional nice properties. With this, (5) leads to a Galois-covariant $\mathfrak{P}$-adic binomial series expansion for $\beta[\Theta]$:

$$\beta[\sigma\Theta] = Y^h \left(1 + \sum_{k=1}^{N-1} \frac{b_k[\sigma\Theta]}{(1-\zeta)^k n^k k!}.(X-1)^k\right) + O(p^{inN}),$$

with $b_k[\sigma\Theta] \in \mathbb{Z}[\zeta]$.

Sketch of the proof that $C = \pm 1$: linear system

We then consider the following linear combination:
$\Delta = \sum_\sigma \lambda_\sigma \cdot \beta[\sigma \cdot \Theta]$ where $\lambda_\sigma \in \mathbb{K}$ verify the linear system:

$$\sum_\sigma \quad \lambda_\sigma \cdot b_k[\sigma \cdot \Theta] = 0, \text{ for } k = 0, \ldots, N-1, \ k \neq \lceil N/2 \rceil \quad \text{and}$$

$$\sum_\sigma \quad \lambda_\sigma \cdot b_{\lceil N/2 \rceil}[\sigma \cdot \Theta] = (1-\zeta)^{\lceil N/2 \rceil} n^{\lceil N/2 \rceil} \lceil N/2 \rceil !.$$

We prove that this system is regular for $N < n-1$ and admits thus a non-null solution. If we let $A = \det\left(b_k[\sigma_c \cdot \Theta]\right)_{k=0;c\in I}^{N-1} \neq 0$, then we observe that $\delta = A.\Delta \in \mathbb{Z}[\zeta]$. We set $N = \lceil n^{3/4} \rceil$ and prove that then, $\delta \neq 0$, but $\delta \equiv 0 \mod p^{in\lceil N/2 \rceil}$. We then bound $\mathbf{N}(\delta)$ by above (using Hadamard's inequality) and by below (using the congruence for δ), and find that

$$p^{n(n-1)N/2} < \mathbf{N}(\delta) < \left(n^{\frac{11}{2}} n^{3/2} + \frac{3}{8} n^{3/4} + \frac{3}{4} \right)^{n-1}$$

This double inequality, combined with (1) of the main theorem, leads to $\log p < 1.64$, which means that the only possibilities for p would be $p = 2, 3$ or 5.

Finally, we rule out the case $p \leq 5$ as follows: in this case, $p \not\equiv \pm 1 \bmod n$ and the decomposition group $D(p)$ contains the automorphism σ_p. We choose thus $\mu = 1 + p\jmath\sigma_p^{-1}$ and proceeding as previously, we build another Θ with the required properties, leading to the double inequality

$$p^{n(n-1)N/2} \leq |\mathbf{N}_{\mathbb{K}/\mathbb{Q}}(\delta)| < \left(n^{4(p+1)+3N^2/2} \cdot N^{N/2+1}\right)^{n-1}.$$

Letting $N = 48$, we obtain the inequality

$$2^n \leq n^{73} \cdot 48^{25/24} < 64n^{73} \quad \Rightarrow \quad \frac{n-6}{73} \leq \log(n)/\log(2),$$

which is false for for $n > 695$, and a fortiori for $n > 163.10^6$. We obtain a contradiction in this case, too. □

Conclusion

- Solutions to the related Diagonal Nagell-Ljunggren equation are upper bounded by relatively small bounds. However, the method we used here is insufficient to raise a final contradiction.
- We proved that binary Thue equations have no solutions for for families of density one of numbers B and n.
- We show the form of the potential solution of binary Thue in the other cases.

Publications

A.Bazso, A.Bérczes, K.Györy and A.Pintér (2010).

On the resolution of equations $Ax^n - By^n = C$ in integers x , y and n $\geq$ 3, II.

Publicationes Mathematicae Debrecen, vol. 76, pp. 227 – 250.

M. A. Bennet (2001).

Rational Approximation To Algebraic Numbers Of Small Height: The Diophantine Equation $|ax^n - by^n| = 1$.

J. Reine Angew. Math., vol. 535, pp. 1–49.

J. P. Buhler and D. Harvey (2011).

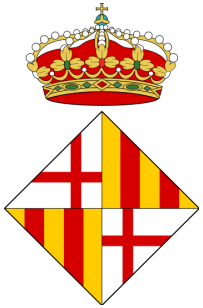
Irregular primes to 163 million.

Mathematics of computation, vol. 80, n 276, pp. 2435 – 2444.

P. Mihăilescu (2008).

Class Number Conditions for the Diagonal Case of the Equation of Nagell and Ljunggren.

Diophantine Approximation, Springer Verlag, Development in Mathematics, vol. 16, pp. 245–273.



Thank you for your attention.