Catalan's Equation Has No New Solution with Either Exponent Less Than 10651

Maurice Mignotte and Yves Roy

CONTENTS

We consider Catalan's equation $x^p - y^q = 1$ (where all variables are integers and p, q are greater than 1), which has the obvious solution $9 - 8 = 1$. Are there others? Applying old and new theoretical results to a systematic computation, we were able to improve on recent work of Mignotte and show that Catalan's equation has only the obvious solutions when $\min\{p, q\} < 10651$. Two crucial tools used are a new result of Laurent, Mignotte, and Nesterenko on linear forms of logarithms, and a criterion obtained by W. Schwarz in 1994.

1. INTRODUCTION AND OVERVIEW

In 1843, Eugène Catalan considered the following question: Are there pairs of consecutive integers that are both powers, other than $(-1, 0)$, $(0, 1)$ and $(8, 9)$? The general opinion, known as Catalan's conjecture, is that the answer is no. Formally, the relevant diophantine equation is $x^m - y^n = 1$, with x, y are integers and m, n integers greater than 1. Of course, we can assume that the exponents are prime numbers, and, possibly after interchanging the two terms on the left, that x and y are both nonnegative. Excluding the trivial case of $x = 1$ and $y = 0$, the equation we are interested in is

$$x^p - y^q = 1, \tag{1.1}$$

where p, q are prime numbers and x, y are integers greater than 1.

The main results toward the verification of Catalan's conjecture are of relatively recent vintage (see [Ribenboim 1994] for a more detailed account). An important step was taken by Tijdeman [1976], who proved that the problem is finite: using Baker's results on linear forms in logarithms, he showed that

1058-6458/96 \$0.50 per page

all unknowns are effectively bounded. The same year, Langevin [1977] obtained the explicit bound 10^{110} for $\max\{p,q\}$, and enormous bounds for x and y. Since then progress on linear forms has led to better bounds. Two years ago, it was possible to prove $\max\{p,q\} < 10^{21}$, and now it seems that $\max\{p,q\} < 10^{18}$ could be proved. However, we shall not pursue upper bounds in the present paper, but will focus our attention on improving the known lower bounds on $\min\{p,q\}$.

The first result in this direction [Nagell 1920] was $\min\{p,q\} \neq 3$. Almost half a century elapsed until Ko Chao proved that $\min\{p,q\} \neq 2$ [Ko 1965]. The best result published since then [Mignotte 1994] had been

$$\min\{p,q\} \geq 13.$$

Here we report a significant advance, proving that

$$\min\{p,q\} \geq 10651.$$

This result was obtained thanks to several theoretical advances and a lot of computation. To explain our strategy, it is convenient to generalize (1.1) slightly to

$$x^p - y^q = \varepsilon, \text{ with } \varepsilon = \pm 1 \text{ and } x, y > 1 \tag{1.2}$$

(still assuming p, q prime). This is so that we can interchange the roles of (x,p) and (y,q) as needed.

The first theoretical advance, discussed in Section 2, is a new lower bound for two linear forms in logarithms [Laurent et al.]. Applied to (1.2) for a fixed prime p, it leads to an upper bound

$$q < q_{\max}(p).$$

We have made great efforts to get a good value for this bound, in order to decrease computation time for the present work and to help the future improvement of upper bounds on $\max\{p,q\}$. In the process (Section 2.1) we present a technical refinement of the congruences obtained in 1964 by Hyyrö.

Then, for a fixed p, we have to consider the range $q < q_{\max}(p)$. For each pair (p,q) we have several theoretical tools to attack (1.2), which in most cases are sufficient to eliminate the possibility of solutions. Specifically, for each prime p one can define two sets $F(p)$ and $H(p)$ such that a solution of (1.2) can only exist for

$$q \in F(p) \cup H(p).$$

The first set corresponds to Fermat quotients:

$$F(p) = \{q : p^{q-1} \equiv 1 \bmod q^2\}.$$

Experiments show that this set is generally very small, but its computation takes a very long time. In our case, to compute all these sets for $p < 10625$ took more than two weeks on a parallel computer with 32 processors. The reason for the strange value 10625 is purely technical: the program was written in C, in double precision, and 10625 is the highest value for which we can compute congruences mod q^2 with this program.

The second set $H(p)$ is related to certain class numbers, and comes from the first general algebraic criterion on Catalan's equation, obtained by Inkeri [1990]. Inkeri's criterion allows us to put

$$H(p) = \{q < q_{\max}(p) : q \text{ divides } h(K'_p)\}, \tag{1.3}$$

where $h(K)$ represents the class number of a number field K and

$$K'_p = \begin{cases} \mathbb{Q}[\sqrt{-p}] & \text{if } p \equiv 3 \bmod 4, \\ \mathbb{Q}[e^{2i\pi/p}] & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

The case $p \equiv 1 \bmod 4$ leads to very serious difficulties; the class number of $\mathbb{Q}[e^{2i\pi/p}]$ is not known for $p \geq 71$. There is a way to overcome this problem: Given q, and setting $h_p = h\big(\mathbb{Q}[e^{2i\pi/p}]\big)$, there are procedures that output either the answer "q does not divide h_p" or "q may divide h_p". But these procedures are very slow. In April 1993, Mignotte [1995] was able to replace the field K'_p in the previous criterion by

$$K_p = \text{the subfield of } \mathbb{Q}[e^{2i\pi/p}] \text{ of degree } 2^d,$$

where 2^d is the maximal power of 2 in $p-1$. For many values of p the degree of this new field K_p is much smaller than $p-1$, and $h(K_p)$ can be easily computed. But there are still difficult examples, like $p = 257$, where this degree is 256.

The newest result we use is from [Schwarz 1995], to the effect that in (1.3) we can replace $h(K_p)$ by $h^-(K_p)$, the relative class number of K_p over K_p^+ (that is, the quotient $h(K_p)/h(K_p^+)$; here K_p^+ is the maximal real subfield of K_p). This represents an enormous progress from the computational point of view: one can compute $h^-(K_p)$ for any p [Washington 1982]. Without this improvement we had serious computational difficulties to get $\min\{p, q\} > 570$, whereas now the most expensive computational step is computing the Fermat quotients.

To summarize the discussion so far, we eliminate most possibilities for (p, q) by using the bound $q < q_{\max}(p)$ and the following fact:

Criterion 1.1. *Let p and q be odd prime numbers. Let $p - 1 = 2^d l$, where l is odd. Let $K = K_p$ be the subfield of $\mathbb{Q}[e^{2i\pi/p}]$ of degree 2^d. Denote by h_K^- the relative class number of K over K^+. Then* (1.2) *has no solution when both of these relations are satisfied*:

$$q \nmid h_K^- \quad \textit{and} \quad p^{q-1} \not\equiv 1 \bmod q^2.$$

Now suppose that, for a given p, we want to analyze a value of q that does not satisfy Criterion 1.1 (that is, $q \in F(p) \cup H(p)$). We have two ways of attack. The more natural, and generally quicker, way is to try Criterion 1.1 on the pair (q, p). We illustrate with the first values of p. For $p = 5$, we have $q_{\max}(5) = 110000$, $F(5) = \{20771, 40487\}$, and $H(5) = \varnothing$; we therefore consider $p = 20771$ and $p = 40487$, and examine the possibility of $q = 5$. Since

$$5 \notin F(20771), \quad 5 \notin H(20771) = \{41\},$$
$$5 \notin F(40487), \quad 5 \notin H(40487) = \{179\},$$

we conclude that (1.2) has no solution when $p = 5$. Similarly, for $p = 7$, we have $q_{\max}(7) = 110000$, $F(7) = \{5\}$, and $H(7) = \varnothing$; since we already know that $p = 5$ leads to no solution, we conclude that $p = 7$ also leads to no solution.

Sometimes this strategy fails; the smallest example, already noticed by Inkeri [1964], is the pair $(p, q) = (83, 4871)$, because

$$4871 \in F(83) \quad \text{and} \quad 83 \in F(4871).$$

In such cases, we try to use the following elementary criterion from [Mignotte 1993]:

Criterion 1.2. *Let p and q be odd prime numbers, and let l be a prime number such that $l = hpq + 1$, with h a positive integer. Let a and b be integers such that $ap \equiv 1 \bmod l$ and $bq \equiv 1 \bmod l$. Then* (1.2) *has no solution when all the following relations are satisfied*: $q^{hq} \not\equiv 1 \bmod l$, $p^{hp} \not\equiv 1 \bmod l$, *and*

$$\left((1 + ag^{jq})^p - 1\right)^{hp} \not\equiv 1 \bmod l$$

for all $j \in \{0, 1, \ldots, hp-1\}$, where g is a primitive root mod l.

For all pairs (p, q) unresolved by the use of Criterion 1.1 (with $p < 10651$), the use of Criterion 1.2 was sufficient to show the absence of solutions, except for the pair (2903, 18787). This last case could be solved by congruences mod 327231967 applied to the formulas obtained during the proof of the first criterion of Inkeri; the details are too technical to be given here.

The conclusion of our computations is, therefore:

Theorem 1.3. *Catalan's equation*

$$x^p - y^q = 1,$$

where p and q are primes and $x, y > 1$ are integers, has no solutions other than $9 - 8 = 1$ when $\min\{p, q\} < 10651$.

The computed data can be obtained from the authors.

In Section 2 we derive the bound $q < q_{\max}(p)$ that makes the problem tractable. In Section 3 we present a result that is not used in the proof of Theorem 1.3, but shows that the special case of Catalan's equation with exponents congruent to 3 mod 4 could be simpler than the general case.

2. BOUNDING ONE EXPONENT AS A FUNCTION OF THE OTHER

Arithmetical Relations

Suppose (x, y, p, q) is a solution to Catalan's equation (1.2). Cassels [1960] proved that there exist integers r and s such that

$$y+\varepsilon=\frac{s^p}{q} \quad \text{and} \quad x-\varepsilon=\frac{r^q}{p}.$$

According to [Hyyrö 1964], there exist also integers $a_0 \geq 1$ and $u_0 \geq 2$ such that $a = qa_0 - \varepsilon$ and $u = p^{q-1}u_0 + 1$ satisfy

$$x-\varepsilon=p^{q-1}a^q \quad \text{and} \quad x^p-\varepsilon=(pua)^q.$$

(Hyyrö gives additional relations satisfied by these numbers, but we will not need them.)

Since $u > 2p^{q-1}$, we get

$$x^p-\varepsilon>(2p^q a)^q \geq \bigl(2p^q(q-1)\bigr)^q,$$

so that

$$x^p \geq \bigl(2(q-1)p^q\bigr)^q. \tag{2.1}$$

This implies

$$r^q=p(x-\varepsilon)>x-1 \geq \bigl((q-1)p^q\bigr)^{q/p} \geq p^{q^2/p},$$

whence

$$\log r>\frac{q}{p}\log p. \tag{2.2}$$

This lower bound seems to be new. In any case, it is quite useful for the estimates in the remainder of this section.

A Crude Bound

It is easy to prove that $s \leq 4^{1/p}q^{1/q}r$ and $r \leq 4^{1/p}p^{1/p}s$, and also that the linear form

$$\Lambda=p\log p-q\log\frac{qr^p}{s^p-q\varepsilon}$$

satisfies $0<|\Lambda| \leq 4p^2r^{-q}$. Let's assume that

$$q>\max\bigl\{400\,p\log p,\ 90000\log p\bigr\}. \tag{2.3}$$

Combined with (2.2), this implies

$$\log|\Lambda| \leq -0.999999\,q\log r. \tag{2.4}$$

We shall apply the following result from [Laurent et al.], where, for α an algebraic number, $h(\alpha) = \log M(\alpha)/\deg\alpha$ is the logarithmic height of α (here $M(\alpha)$ is the Mahler measure of α, the definition of which is recalled on page 267).

Theorem 2.1. *Let α_1, α_2 be two multiplicatively independent algebraic numbers with $|\alpha_1|$, $|\alpha_2| \geq 1$, and let $\log\alpha_1$ and $\log\alpha_2$ be any determination of their logs. Put*

$$\Lambda=b_2\log\alpha_2-b_1\log\alpha_1,$$

where b_1 and b_2 are positive integers. Put

$$D=\frac{[\mathbb{Q}(\alpha_1,\alpha_2):\mathbb{Q}]}{[\mathbb{R}(\alpha_1,\alpha_2):\mathbb{R}]}.$$

Let K be an integer ≥ 2, let L, R_1, R_2, S_1, S_2 be positive integers, and let $\rho > 1$ be a real number. Suppose that

$$R_1S_1 \geq L \quad \text{and} \quad R_2S_2>(K-1)L. \tag{2.5}$$

Put $R = R_1 + R_2 - 1$, $S = S_1 + S_2 - 1$,

$$g=\frac{1}{4}-\frac{KL}{12\,RS}, \tag{2.6}$$

and

$$b=\bigl((R-1)b_2+(S-1)b_1\bigr)\biggl(\prod_{k=1}^{K-1}k!\biggr)^{-2/(K^2-K)}.$$

Suppose also that

$$(\rho-1)\log\alpha_i+2Dh(\alpha_i) \leq a_i \quad \textit{for } i=1,2,$$

that the numbers $rb_2 + sb_1$, for $0 \leq r \leq R-1$ and $0 \leq s \leq S-1$, are pairwise distinct, and that

$$K(L-1)\log\rho-(D+1)\log KL$$
$$-D(K-1)\log(b/2)-gL(Ra_1+Sa_2)>0. \tag{2.7}$$

Then we have the lower bound

$$|\Lambda'| \geq \rho^{-KL+\frac{1}{2}}, \tag{2.8}$$

where

$$\Lambda'=\Lambda\max\biggl\{\frac{LSe^{LS|\Lambda|/(2b_2)}}{2b_2},\ \frac{LRe^{LR|\Lambda|/(2b_1)}}{2b_1}\biggr\}. \quad \square$$

Before applying Theorem 2.1, we apply a corollary of it [Laurent et al., Corollary 2], which is weaker but much simpler to use.

Corollary 2.2. *With the notations of Theorem* 2.1, *suppose moreover that* α_1 *and* α_2 *are positive real numbers. Then*

$$\log|\Lambda| \geq -24.34\, D^4 \Big(\max\Big\{\log b' + 0.5,\, \frac{21}{D}\Big\}\Big)^2 \log A_1 \log A_2,$$

where

$$\log A_i \geq \max\left\{\frac{1}{D},\, \frac{|\log\alpha_i|}{D},\, h(\alpha_i)\right\} \quad \textit{for } i = 1,\, 2,$$

and $b' = \dfrac{b_1}{\log A_2} + \dfrac{b_2}{\log A_1}$. □

We apply the corollary with $b_1 = q$, $b_2 = p$,

$$\alpha_1 = \frac{qr^p}{(s^p - \varepsilon q)},$$

$\alpha_2 = p$, and $D = 1$. Notice that α_1 and α_2 are multiplicatively independent: otherwise Λ would be an integer times $\log p$, contradicting the trivial estimate $0 < |\Lambda| < 1$.

Notice also that

$$|\log\alpha_1| \leq \frac{p\log p}{q} + \frac{|\Lambda|}{q} \leq \frac{p}{q}\log(p+1).$$

Moreover,

$$\begin{aligned} h(\alpha_1) &\leq \max\big\{p\log r + \log q,\, \log(s^p + q)\big\} \\ &\leq \max\big\{(p+1)\log r,\, p\log s + 2^{-p}\big\} \\ &\leq (p+1)\log r, \end{aligned}$$

since $q \leq s$. Clearly, $\log\alpha_2 = h(\alpha_2) = \log p$. Thus we can apply Corollary 2.2 with

$$\log A_1 = (p+1)\log r \quad \text{and} \quad \log A_2 = \log p.$$

(Note that to apply Corollary 2.2 we only have to choose $\log A_1$ and $\log A_2$. Then b' is defined in terms of b_1, b_2, $\log A_1$ and $\log A_2$. The corollary gives a lower bound for Λ depending only on these previous quantities and on D.)

Hence, by (2.3), we have

$$b' = \frac{q}{\log p} + \frac{p}{(p+1)\log r} \leq \frac{1.001\, q}{\log p}.$$

We get

$$\log|\Lambda| \geq -24.34\big(\max\{21,\, \log(q/\log p) + 0.51\}\big)^2 \times (p+1)\log p \log r.$$

Comparing this inequality with (2.4) leads to

$$q \leq 24.4\,(p+1)\log p\big(\max\{21,\, \log(q/\log p) + 0.51\}\big)^2. \tag{2.9}$$

In particular, $q \leq 170000$ for $p \leq 7$.

A Sharper Bound

In this section we assume $p \geq 11$. We can apply Theorem 2.1 with

$$a_1 = 2(p+1)\Big(1 + \frac{(\rho-1)}{4q}\Big)\log r$$

and $a_2 = (\rho+1)\log p$. We shall take $17 \leq \rho \leq 25$. By (2.2) and (2.3), we have $a_1 > 2q\log p$, so that $a_1 > 1.03 \times 10^5$, $a_2 > 43.16$, and $a_1 a_2 > 3.51 \times 10^7$. Then, to satisfy condition (2.5), we take

$$\begin{aligned} R_1 &= 1, \quad S_1 = L, \\ R_2 &= \big[\sqrt{(K-1)La_2/a_1}\,\big] + 1, \\ S_2 &= \big[\sqrt{(K-1)La_1/a_2}\,\big] + 1. \end{aligned}$$

We suppose that $7 \leq L \leq 5\log p$. We take $K = [\mu^2 L a_1 a_2] + 1$, where μ is some real number to be chosen later, satisfying $0.2 \leq \mu \leq 0.5$; thus

$$K \geq 0.2^2 \times 7 \times 1.03 \times 10^6 \times 43.16 > 1.24 \times 10^7.$$

If there exist two integers r_0 and s_0, with $|r_0| < R$ and $|s_0| < S$, such that $r_0 b_2 + s_0 b_1 = 0$, then q divides r_0, so that

$$\begin{aligned} q &< R \leq 1.5\,\mu L(\rho+1)p \\ &< 1.5 \times 0.5 \times 5 \times 26 \times p\,\log p < 100\,p\,\log p, \end{aligned}$$

which contradicts (2.3). Hence, the numbers

$$rb_2 + sb_1,$$

for $0 \leq r \leq R-1$ and $0 \leq s \leq S-1$, are pairwise distinct.

We have the following general upper bound for b [Laurent et al., Lemma 6]:

$$b \le \frac{\big((R-1)b_2+(S-1)b_1\big)}{K-1} \times \exp\Big(\tfrac{3}{2}-\frac{\log(2\pi(K-1)/\sqrt{e})}{K-1}+\frac{\log K}{6K(K-1)}\Big).$$

Thanks to our hypotheses on L and K, this leads to

$$\begin{aligned}\log b &\le 1.5+\log\big(\sqrt{L}(\sqrt{K}+1)(b_1\sqrt{a_1/a_2}+b_2\sqrt{a_2/a_1})\big) -\log(K-1)-\frac{\log(3.8\,K)}{K-1}\\ &\le 1.5+\log\Big(\frac{\sqrt{L}\sqrt{a_1a_2}}{(\rho+1)(\sqrt{K}-1)}\Big)+\log b'-\frac{\log(3.8\,K)}{K-1}\\ &\le 1.5-\log\big((\rho+1)\mu\big)+\log b'+\frac{1}{\sqrt{K-1}}-\frac{\log(3.8\,K)}{K-1}\\ &\le 1.5-\log((\rho+1)\mu)+\log\frac{q}{\log p} +\frac{(\rho+1)p}{2q^2}+\frac{1}{\sqrt{K-1}}-\frac{\log(3.8\,K)}{K-1},\end{aligned}$$

since now

$$b' = (\rho+1)\Big(\frac{b_1}{a_2}+\frac{b_2}{a_1}\Big) \le \frac{q}{\log p}+\frac{p(\rho+1)}{2\,(p+1)\log r} \le \frac{q}{\log p}\Big(1+\frac{(\rho+1)p}{2q^2}\Big).$$

Now we consider the quantity g of (2.6). From the relations

$$R = R_1+R_2-1 \le \sqrt{(K-1)La_2/a_1},$$
$$S = S_1+S_2-1 \le L+\sqrt{(K-1)La_1/a_2},$$

we get

$$\begin{aligned} gL(Ra_1+Sa_2) &= \tfrac14 L(Ra_1+Sa_2)-\frac{KL^2}{12}\Big(\frac{a_1}{S}+\frac{a_2}{R}\Big) \qquad (2.10)\\ &\le \tfrac14 L^2a_2+\tfrac12 L^{3/2}\sqrt{(K-1)a_1a_2}-\frac{KL^2}{12}\Big(\frac{a_1}{S}+\frac{a_2}{R}\Big).\end{aligned}$$

We have

$$\frac{1}{R} \ge \frac{1}{\sqrt{(K-1)La_2/a_1}},$$

and the identity

$$\frac{1}{x+y}=\frac1x-\frac{y}{x^2}+\frac{y^2}{(x+y)x^2}$$

implies

$$\frac1S \ge \frac{1}{\sqrt{(K-1)La_1/a_2}}-\frac{L}{(K-1)La_1/a_2} +\frac{a_2L^2}{a_1(K-1)L\big(L+\sqrt{(K-1)La_1/a_2}\,\big)}.$$

Hence we obtain the lower bound

$$\begin{aligned} KL^2\Big(\frac{a_1}{S}+\frac{a_2}{R}\Big) &\ge (K-1)L^2\Big(\frac{a_1}{S}+\frac{a_2}{R}\Big)\\ &\ge 2L^{3/2}\sqrt{(K-1)a_1a_2}-a_2L^2 +\frac{a_2L^3}{L+\sqrt{(K-1)La_1/a_2}}.\end{aligned}$$

Plugging this into (2.10) gives

$$gL(Ra_1+Sa_2) \le \tfrac13 L^{3/2}\sqrt{(K-1)a_1a_2} +\tfrac13 L^2a_2-\frac{a_2L^3}{12\big(L+\sqrt{(K-1)La_1/a_2}\,\big)}.$$

Ignoring the last term, we get

$$gL(Ra_1+Sa_2) \le \tfrac13 L^{3/2}\sqrt{(K-1)a_1a_2}+\tfrac13 a_2L^2.$$

Besides, since $\log r > (q/p)\log p$, we have

$$\frac{a_2}{a_1} \le \frac{(\rho+1)\log p}{2(p+1)\log r} < \frac{(\rho+1)\log p}{2(p+1)(q/p)\log p} < \frac{\rho+1}{2\,q}.$$

Using these remarks, we see that condition (2.7) is satisfied if, putting $\lambda=\log\rho$, we have

$$\begin{aligned} 0 < {} & K(L-1)\lambda+(K-1)\log 2-2\log(KL) -\tfrac13 L^{3/2}\sqrt{(K-1)a_1a_2}-\tfrac13 a_2L^2\\ & -(K-1)\Big(1.5-\log((\rho+1)\mu)+\log\Big(\frac{q}{\log p}\Big) +\frac{(\rho+1)p}{2q^2}+\frac{1}{\sqrt{K-1}}-\frac{\log(3.8\,K)}{K-1}\Big). \qquad (2.11)\end{aligned}$$

Now the right-hand side of (2.11) is greater than or equal to $\Phi+\Theta$, where

$$\Phi = K(L-1)\lambda+K\log 1.999-\tfrac13 L^{3/2}\sqrt{(K-1)a_1a_2} -(K-1)\Big(1.5-\log\big((\rho+1)\mu\big)+\log\Big(\frac{q}{\log p}\Big)\Big)$$

and

$$\Theta = 5K \times 10^{-4} - \log(KL^2) - K\frac{(\rho+1)p}{q^2} - \sqrt{K} - \tfrac{1}{3}a_2L^2.$$

It is easy to verify that Θ is positive. Indeed,

$$\frac{(\rho+1)p}{q^2} \le \frac{26}{90000 \times 400 \times \log^2 p} < 2 \times 10^{-7},$$
$$\frac{\sqrt{K}}{K} \le 2.84 \times 10^{-4},$$
$$\frac{\log(KL^2)}{K} < 3\frac{\log K}{K} < 4 \times 10^{-6},$$
$$\frac{\frac{1}{3}a_2L^2}{K} \le \frac{a_2L^2}{35^2La_1a_2} = \frac{L}{35^2a_1} \le \frac{5\log p}{6 \times 0.2^2 \times q\log p} < \frac{5}{6 \times 0.2^2 \times 200000} < 1.1 \times 10^{-4},$$

so $\Theta \ge K(5-4.6) \times 10^{-4} > 0$. Then, dividing Φ by La_1a_2, we see that condition (2.7) is satisfied when

$$\mu\Big((L-1)\lambda + \log 1.999 - 1.5 + \log(\rho+1) - \log\frac{q}{\log p}\Big) + \mu\log\mu - \tfrac{1}{3}L \ge 0. \quad (2.12)$$

In such a case, by (2.8) and the inequality $R+S \le K$, we get

$$\log|\Lambda| \ge -KL\log\rho - \log(KL).$$

Comparing this inequality with (2.4) gives

$$q \le 2.0001\,\mu^2L^2(\rho+1)(p+1)\log p\log\rho.$$

Now we can describe the procedure used to get an upper bound $q_{\max}(p)$ for the exponent q in (1.2), when p is fixed. We first apply condition (2.9) to get a first upper bound, say q_0, for this exponent. Then, for a suitable choice of ρ and L, we use this upper bound to find a value μ for which (2.11) holds. Then (2.11) gives an upper bound $q_1 \le q_0$. If $q_1 < q_0$ we repeat this process using the new upper bound q_1 and some choice of ρ and L (possibly the same as before), which gives an upper bound $q_2 \le q_1$. We continue in this way, and stop after a certain number of tries, obtaining a value q_∞. Finally we take

$$q_{\max}(p) = \max\big\{90000\,\log p,\ 400\,p\,\log p,\ q_\infty\big\},$$

in order to respect (2.3). Notice that $q_{\max}(p) = 90000\,\log p$ for $p \le 53$.

Since $\lambda = \log p$, condition (2.12) is equivalent to

$$\mu\Big(L\log\rho - \theta + \log\Big(1+\frac{1}{\rho}\Big) - \log\frac{q}{\log p}\Big) + \mu\log\mu - \tfrac{1}{3}L \ge 0,$$

where we put $\theta = 1.5 - \log 1.999$. This can also be written as

$$L(\mu\log\rho - \tfrac{1}{3}) \ge \mu\Big(\theta - \log\Big(1+\frac{1}{\rho}\Big) + \log\frac{q}{\log p}\Big).$$

We choose

$$\mu = \frac{2}{3\log\rho};$$

then the previous condition becomes

$$L \ge 3 \times \frac{2}{3\log\rho}\Big(\theta - \log\Big(1+\frac{1}{\rho}\Big) + \log\frac{q}{\log p}\Big).$$

For $\rho = 22.9$ (so that $\mu = 0.2129\ldots \in [0.2, 0.5]$), we find that this inequality holds if

$$L \ge 0.6388(\log q - \log\log p + 0.765),$$

and we can take

$$L = [0.6388\log(q/\log p) + 1.49].$$

(We verify the condition $7 \le L \le 5\log p$. From (2.3), we have

$$L \ge 0.6388\log 90000 > 7.$$

Put $z = q/\log p$; then (2.3) implies $z > 11.407$ and

$$\max\{21,\ \log(q/\log p) + 0.51\} < 1.841\,z;$$

thus (2.9) gives

$$z \le 24.4 \times 1.841^2\,(p+1)\log^2 z,$$

which leads to

$$\log z < \log 82.7 + \log(p+1) + 2\log\log z$$

and

$$\log z < 1.746\,\log\big(82.7\,(p+1)\big).$$

Then an elementary numerical study shows that $L < 4\log p$ for $p \geq 11$. This ends the verification.)

Thus we get

$$q \leq 6.7853\,(p+1)\big(0.6388\log(q/\log p)+1.49\big)^2 \log p,$$

which implies

$$q \leq 2.769\,(p+1)\big(\log(q/\log p)+2.333\big)^2 \log p \quad (2.13)$$

for $p \geq 11$; thus

$$q \leq 2.77\,p\big(\log(q/\log p)+2.333\big)^2 \log p \quad (2.14)$$

for $p \geq 3000$.

On the range $11 \leq p < 10651$, we have computed the best possible value $q_{\max}(p)$ obtained by Theorem 2.1. Inequality (2.14) is given as a reference for possible further computations. Example: for $p < 10^4$ we have $q_{\max}(p) < 8.7 \times 10^7$.

3. AN APPLICATION OF INKERI'S FIRST CRITERION

We now prove a result that is not used in the proof of Theorem 1.3, but shows that the special case of Catalan's equation with exponents congruent to 3 mod 4 could be simpler than the general case.

Instead of (1.2) we will work with the equation $x^p - y^q = 1$, where $q > p > 1$ are positive integers and x, y are (possibly negative) integers with $|x|$, $|y| > 1$. We will in fact assume that $p > 50$.

We recall briefly the work in [Inkeri 1964]. For p prime, with $p \equiv 3 \bmod 4$, suppose that a runs over the quadratic residues mod p and that b runs over the nonresidues. Put

$$A(X) = \prod_a (X - \zeta^a), \quad B(X) = \prod_b (X - \zeta^b),$$

where $\zeta = e^{2i\pi/p}$. Then

$$4\,\frac{X^p - 1}{X - 1} = 2\,A(X)\cdot 2\,B(X) = Y^2(X) + pZ^2(X),$$

where

$$Y(X) = A(X) + B(X),$$
$$Z(X) = \big(B(X) - A(X)\big)/\sqrt{-p}.$$

The polynomials Y and Z have integer coefficients. Clearly, $\deg Y = \frac{1}{2}(p-1)$ and

$$Y(X) = 2X^{(p-1)/2} + \cdots,$$
$$L(Y) \leq L(A) + L(B) \leq 2^{(p+1)/2},$$

where $L(P)$ denotes the length of the polynomial P (that is, the sum of the modules of its coefficients).

From the formula on Gauss sums,

$$\sum_a \zeta^a - \sum_b \zeta^b = \sqrt{-p},$$

we see that $\deg Z = \frac{1}{2}(p-3)$ and that

$$Z(X) = X^{(p-3)/2} + \cdots,$$
$$L(Z) \leq \big(L(A) + L(B)\big)/\sqrt{p} \leq 2^{(p+1)/2}/\sqrt{p}.$$

Now, by Hyyrö's theorem (see the beginning of Section 2), there exist integers a and u such that

$$|x| - 1 = p^{q-1}a^q \quad \text{and} \quad |x|^p - 1 = (|x|-1)pu^q.$$

Thus $4pu^q = Y^2 + pZ^2$ and, if $Y_1 = Y/(2p)$ and $Z_1 = \frac{1}{2}Z$, then

$$u^q = (Z_1 + Y_1\sqrt{-p})(Z_1 - Y_1\sqrt{-p});$$

moreover Y_1 and Z_1 are coprime integers [Inkeri 1964]. In the quadratic field $\mathbb{Q}(\sqrt{-p})$, this implies a relation

$$(Z_1 + Y_1\sqrt{-p}) = \mathfrak{b}^q,$$

where $\mathfrak{b}$ is some ideal of this field. If we assume that q does not divide the class number of $\mathbb{Q}(\sqrt{-p})$, there exists an algebraic integer β, belonging to this field, such that

$$Z_1 + Y_1\sqrt{-p} = \beta^q.$$

Hence, $\beta^q - \bar\beta^q = 2Y_1\sqrt{-p}$ and $\beta^q + \bar\beta^q = 2Z_1$. Put $\beta = |\beta|e^{i\theta}$, with $|\theta| \leq \pi$. Then

$$\cot(q\theta) = i\,\frac{\beta^q + \bar\beta^q}{\beta^q - \bar\beta^q} = \frac{Z(|x|)\sqrt{p}}{Y(|x|)}.$$

Using the previous estimates relative to Y and Z, we get

$$|\cot(q\theta)| < \sqrt{p}\,\frac{|x|^{(p-3)/2} + 2^{(p+1)/2}|x|^{(p-5)/2}}{2|x|^{(p-1)/2} - 2^{(p+1)/2}|x|^{(p-3)/2}} = \sqrt{p}\,\frac{1 + 2^{(p+1)/2}/|x|}{2|x|\big(1 - 2^{(p+1)/2}/|x|\big)} < \frac{2\sqrt{p}}{3|x|},$$

since $|x| > p^p$ by an argument like the one leading to (2.1). Thus there exists an integer k such that the linear form $\Lambda := ki\pi - q(2i\theta)$ satisfies

$$|\Lambda| < \frac{2\sqrt{p}}{|x|}.$$

We now use [Laurent et al., Theorem 3]:

Theorem 3.1. *Let α be an algebraic number of modulus 1 that is not a root of unity, let b_1 and b_2 be two positive integers, and set $\Lambda = b_1 i\pi - b_2 \log\alpha$. Put $D = \frac{1}{2}[\mathbb{Q}(\alpha) : \mathbb{Q}]$,*

$$t \geq \max\big\{20,\ 12.85\ |\log\alpha| + Dh(\alpha)\big\},$$
$$H = \max\Big\{17,\ D\log\Big(\frac{b_1}{2a} + \frac{b_2}{25.7\pi}\Big) + 4.6D + 3.25\Big\}.$$

Then $\log|\Lambda| \geq -9tH^2$. □

In our case we take $b_1 = k$, $b_2 = q$, $\alpha = \beta/\bar{\beta} = e^{2i\theta}$, and $D = 1$.

For an algebraic number γ, let $M(\gamma)$ denote the Mahler measure of γ, that is, the product

$$|a_0| \prod_{j=1}^{d} \max\{1,\ |\gamma_j|\},$$

where a_0 is the leading coefficient and the γ_j the roots of an irreducible polynomial with integer coefficients of which γ is a root. We have the estimates

$$M(\alpha) = |\beta|^2 \leq (|Z_1| + |Y_1|\sqrt{p})^{2/q} \leq \big(x^{(p-1)/2}\big)^{2/q} = x^{(p-1)/q},$$

or, in terms of the height,

$$h(\alpha) \leq \frac{p-1}{2q}\log x.$$

This implies, with the notation of Theorem 3.1, that

$$12.85 \times 2\pi + \frac{p-1}{2q}\log x < \frac{p}{2q}\log x;$$

indeed, (2.1) says that $|x| > p^{q^2/p}$, so that

$$\frac{1}{2q}\log|x| > 12.85 \times 2\pi$$

because of (2.3). Thus we can take

$$t = \frac{p}{2q}\log x$$

(which implies $t > \frac{1}{2}q\log p$), and then we have

$$H \leq \max\big\{17,\ \log q + 3.46\big\}.$$

(Proof: We have $0 < k < q$ and $t > \frac{1}{2}q\log p$, so

$$D\log\Big(\frac{b_1}{2a} + \frac{b_2}{25.7\pi}\Big) + 4.6D + 3.25 < \log\Big(\frac{q}{25.7\,\pi}\Big) + \frac{25.7\,\pi}{2a} + 7.85 < 3.459,$$

which proves that $H \leq \max\{17, \log q + 3.46\}$.) Comparing the lower bound of $\log|\Lambda|$ with its upper bound, after some easy simplifications, we get

$$q \leq 4.51\,pH^2 = 4.51\,p\,(\max\{17,\ \log q + 3.46\})^2.$$

This upper bound, like (2.13) and (2.14), is derived here as a reference for possible further computations. Note that it is better than (2.13) for $p \geq 31$.

ACKNOWLEDGEMENT

We are very grateful to one of the referees for pointing out several minor mistakes and obscurities and for simplifying considerably the proof of the better bound in Section 2 (pages 263 and following).

REFERENCES

[Cassels 1960] J. W. S. Cassels, "On the equation $a^x - b^y = 1$, II", *Proc. Cambridge Society* **56** (1960), 97–103.

[Hyyrö 1964] S. Hyyrö, "Über das Catalansche Problem", *Ann. Univ. Turku*, Ser. AI **79** (1964), 10 pages.

[Inkeri 1964] K. Inkeri, "On Catalan's problem", *Acta Arith.* **9** (1964), 285–290.

[Inkeri 1990] K. Inkeri, "On Catalan's conjecture", *J. Number Theory* **34** (1990), 142–152.

[Ko 1965] Ko Chao, "On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$", *Sci. Sinica* **14** (1965), 457–460.

[Langevin 1977] M. Langevin, "Quelques applications de nouveaux résultats de van der Poorten", *Sém. Delange–Pisot–Poitou* (1977/78), Paris, Exp. 4, 7 pages.

[Laurent et al.] M. Laurent, M. Mignotte, and Y. Nesterenko, "Formes linéaires en deux logarithmes et déterminants d'interpolation", to appear in *J. Number Theory*.

[Mignotte 1992] M. Mignotte, "Sur l'équation de Catalan", *C. R. Acad. Sci. Paris*, Sér. I **314** (1992), 165–168.

[Mignotte 1993] M. Mignotte, "Un critère élémentaire pour l'équation de Catalan", *C. R. Math. Rep. Acad. Sci. Canada* **15** (1993), 199–200.

[Mignotte 1994] M. Mignotte, "Sur l'équation de Catalan (II)", *Theoret. Comp. Sci.* **123** (1994), 145–149.

[Mignotte 1995] M. Mignotte, "A criterion on Catalan's equation", *J. Number Theory* **52** (1995), 280–283.

[Nagell 1920] "Des équations indéterminées $x^2+x+1 = y^n$ et $x^2+x+1 = 3y^n$", *Nordsk. Mat. Forenings*, Skr. (1) **2** (1920), 14 pages.

[Ribenboim 1994] P. Ribenboim, *Catalan's conjecture*, Academic Press, Boston, 1994.

[Tijdeman 1976] R. Tijdeman, "On the equation of Catalan", *Acta Arith.* **29** (1976), 197–209.

[Schwarz 1995] W. Schwarz, "A note on Catalan's equation", *Acta Arith.* **72** (1995), 277–279.

[Washington 1982] L. C. Washington, *Introduction to cyclotomic fields*, Springer, New York, 1982.

Maurice Mignotte, Université Louis Pasteur, Centre de Calcul de l'Esplanade, 7, rue René Descartes, F-67084 Strasbourg, France (mignotte@math.u-strasbg.fr)

Yves Roy, Université Louis Pasteur, Centre de Calcul de l'Esplanade, 7, rue René Descartes, F-67084 Strasbourg, France (yr@dept-info.u-strasbg.fr)

Received December 27, 1994; accepted in revised form August 8, 1995