Publ. Math. Debrecen
79/3-4 (2011), 269–282
DOI: 10.5486/PMD.2011.5040

On the Diophantine equation $x^4 - q^4 = py^r$

By AURÉLIEN BAJOLET (Talence), BENJAMIN DUPUY (Talence),
FLORIAN LUCA (Michoacán) and ALAIN TOGBÉ (Westville)

To Professors K. Győry, A. Pethő, J. Pintz and A. Sárközy on their birthdays

Abstract. In this paper, we characterize up to finitely many exceptions all the solutions of the Diophantine equation $x^4 - q^4 = py^r$ with $r > 3$ a fixed prime. When $r = 5$, we show that there are no exceptions.

1. Introduction

Let $r \geq 3$ be a fixed prime. Consider the Diophantine equation

$$x^4 - q^4 = py^r, \tag{1}$$

in prime unknowns p, q and integer unknown x coprime to q. The case $r = 3$ has been treated in [16]. Here, we present the following more general result.

Theorem 1. *For every fixed prime $r > 3$, all but finitely many solutions (x, y, p, q) of equation (1) with p and q primes and positive integer x coprime to q are of the form*

$$x = a^r + 4b^r, \quad q = |a^r - 2^{r-3}b^r|, \quad pc^r = a^{2r} + 2^{2r-6}b^{2r}, \quad \text{and} \quad y = 2abc \tag{2}$$

for some integers a, b, and c.

Mathematics Subject Classification: 11D41, 11Y16.
Key words and phrases: exponential Diophantine equations.

Taking $b = c = 1$, SCHINZEL's Hypothesis H [23], and, more generally, the BATEMAN–HORN conjectures [2], imply that there should be infinitely many integers a such that $a^r - 2^{r-3}$ and $a^{2r} + 2^{2r-6}$ are simultaneously prime numbers. This is simply because the polynomials $X^r - 2^{r-3}$ and $X^{2r} + 2^{2r-6}$ are both irreducible when $r > 3$ is prime and can represent simultaneously integers coprime to all primes up to $2r$. Hence, the Diophantine equation (1) should have infinitely many solutions (x, y, p, q) satisfying the given primality and coprimality conditions.

We also treat the particular case $r = 5$ which has been investigated in the recent paper [22], where it was shown that it has no solutions under various restrictions on the unknowns x, y, p and q. However, trying out some particular values for (a, b, c) in the parametrization (2) with $r = 5$ such as $(a, b, c) = (1, 1, 1)$, $(5, 3, 1)$, $(73, 3, 1)$, we get some solutions like

$$\begin{aligned} 5^4 - 3^4 &= 17 \cdot 2^5, \\ 4097^4 - 2153^4 &= 10710409 \cdot 30^5, \\ 2073072565^4 - 2073070621^4 &= 4297625829704502433 \cdot 438^5. \end{aligned} \tag{3}$$

The following result shows that when $r = 5$ there are no exceptions to the parametrization (2).

Theorem 2. *When $r = 5$, all solutions of equation* (1) *are given by the parametrization* (2).

2. The proofs

We first prove Theorem 1 and then prove Theorem 2.

PROOF OF THEOREM 1. If $p = 2$, then x and q are odd, therefore $16 \mid x^4 - q^4$. Thus, y is even. We then get that

$$x + \varepsilon q = 2^{r-1} u_1^r, \qquad x - \varepsilon q = 2u_2^r, \qquad x^2 + q^2 = 2u_3^r$$

for $\varepsilon \in \{\pm 1\}$, some integers u_1, u_2, u_3 with the last two odd such that $2u_1u_2u_3 = y$. Eliminating x and q leads to equation

$$u_2^{2r} + 2^{2r-4} u_1^{2r} = u_3^r, \tag{4}$$

which has no nonzero integer solutions by Theorem 3 in [19]. So, from now on, we assume that p is odd.

If $q = 2$, then x is odd and we are led to either $x^2 + 4 = y_1^r$, or $x^2 - 4 = y_1^r$. Clearly, $x \geq 5$. The first equation has no solutions by the results from [15], while the second equation implies $x - 2 = y_2^r$ and $x + 2 = y_3^r$ so that

$$4 = y_3^r - y_2^r = (y_3 - y_2)(y_3^{r-1} + \cdots + y_2^{r-1}) > 3^{r-1} > 4,$$

where the last inequalities above follow because $y_2 < y_3$ are both odd positive integers. This is a contradiction.

Assume next that $q > 2$ and that x is even. If p divides $x^2 + q^2$, it follows that both relations $x - q = y_1^r$ and $x + q = y_2^r$ hold with two odd integers y_1 and y_2. Thus,

$$q = \frac{1}{2}(y_2^r - y_1^r),$$

which together with the fact that q is prime implies that $y_2 - y_1 = 2$. Hence, we can write $y_2 = u + 1$ and $y_1 = u - 1$. Then

$$x = \frac{1}{2}((u+1)^r + (u-1)^r), \qquad q = \frac{1}{2}((u+1)^r - (u-1)^r), \tag{5}$$

so

$$x^2 + q^2 = \frac{1}{2}((u+1)^{2r} + (u-1)^{2r}) = (u^2+1)\left(\frac{(u+1)^{2r} + (u-1)^{2r}}{(u+1)^2 + (u-1)^2}\right). \tag{6}$$

The two factors on the right above are either coprime, or their greatest common divisor is r. In the second case, r exactly divides the second factor. Since $x^2 + q^2 = py_3^r$, we get that either

$$u^2 + 1 = y_4^r, \tag{7}$$

or

$$u^2 + 1 = r^{r-1} y_4^r. \tag{8}$$

The first case (7) appears either if $p = r$ or if the two factors on the right–hand side of (6) are coprime, and the second case appears in the remaining instance. The equation (7) has no positive integer solutions (u, y_4). Indeed, this is a particular case of the Catalan equation and was solved by Lebesgue [14] more than 150 years ago. So, one only needs to look at equation (8). Since $r \geq 3$, it follows from known finiteness results concerning integer solutions to hyper-elliptic equations (see [1], [3], [6]–[8], [18], [24]–[26], [30]), that equation (8) has only finitely many integer solutions (u, y_4).

Assume next that x is even but that p divides $x^2 - q^2$. Then $x^2 + q^2 = y_1^r$. Factoring it in $\mathbb{Z}[i]$ leads to an equation of the form

$$x + iq = (u + iv)^r,$$

so

$$q = \frac{1}{2i}((u+iv)^r - (u-iv)^r)).$$

Since q is prime and v divides the integer appearing in the right-hand side above, we get that $v = \pm 1$ or $\pm q$. In the latter case, we are lead to the rth term of the Lucas sequence $(u_n)_{n\geq 0}$ whose roots are $\alpha = u + iv$ and $\beta = u - iv$ being equal to ± 1; that is, $u_r = \pm 1$. This is impossible for $r \geq 5$ by the results from [5].

In the former case, we have

$$x = \frac{1}{2}((u+iv)^r + (u-iv)^r), \quad q = \frac{1}{2i}((u+iv)^r - (u-iv)^r)), \qquad v = \pm 1, \tag{9}$$

so x is a monic polynomial of degree r in u and q is a polynomial of degree $r-1$ in u. Since $x^2 - q^2 = py_2^r$, it follows that

$$\text{either} \quad x + q = y_3^r, \quad \text{or} \quad x - q = y_3^r. \tag{10}$$

However, both $x + q$ and $x - q$ are monic polynomials of degree r in u, therefore the above equations have only finitely many solutions (u, y_3), which can be easily computed using Runge's method (see, for example, [13], [20], [21], [27], [31]).

Finally, assume that x is odd. Suppose first that $x^2 + q^2 = 2y_1^r$. A more general equation was studied by Tengely [29], namely $x^2 + q^{2m} = 2y_1^r$. He proved that this equation has only finitely many solutions if y_1 is not a sum of two consecutive squares. One can also factor the equation $x^2 + q^2 = 2y_1^r$ in $\mathbb{Z}[i]$ to get

$$\begin{aligned} x &= \frac{1}{2}((1+i)(u+iv)^r + (1-i)(u-iv)^r), \\ q &= \frac{1}{2i}((1+i)(u-iv)^r - (1-i)(u+iv)^r), \end{aligned} \tag{11}$$

for some coprime nonzero integers u and v of different parities. Here, $y = u^2 + v^2$. The above expression for q is a homogeneous polynomial in (u, v) of degree r without repeated roots which is a multiple of $u + v$. Since q is prime, we get that $u + v = \pm 1$ or $\pm q$. In the latter case, factoring out $u + v$ from the expression for q we are left with

$$\pm 2i = \frac{(1+i)(u-iv)^r - (1-i)(u+iv)^r}{u+v} \tag{12}$$

and the expression on the right–hand side of formula (12) is a homogeneous polynomial of degree $r - 1 \geq 4$ in (u, v) without multiple roots. Hence, equation (12) is a Thue equation and therefore has only finitely many solutions.

In the former case, we have that $u + v = \pm 1$, so we may assume that both x and q are polynomials in the variable u. Now

$$x^2 - q^2 = 2^{r-1} p y_2^r, \tag{13}$$

so we get that

$$x \pm q = \delta y_3^r, \quad \text{where} \quad \delta \in \{2, 2^{r-2}\}. \tag{14}$$

The expressions $x \pm q$ on the left hand side above are polynomials of degree r in u with simple roots. Hence, we arrive to a collection of finitely many Diophantine equations each having only finitely many integer solutions (u, y_3).

Thus, aside from a total of finitely many possible solutions, we must have that x and q are both odd and that $p \mid x^2 + q^2$. Consequently, for some integers a and b we must have

$$\{x - q, x + q\} = \{2a^r, 2^{r-2} b^r\}.$$

This leads to $x = a^r + 2^{r-3} b^r$, and $q = |a^r - 2^{r-2} b^r|$.

Writing c such that $y = 2abc$, we also get that $2pc^r = x^2 + q^2 = 2(a^{2r} + 2^{2r-6} b^{2r})$, so $pc^r = a^{2r} + 2^{2r-6} b^{2r}$.

This leads to the desired conclusion and completes the proof of Theorem 1. □

Proof of Theorem 2. For the proof of Theorem 2, we go back to the previous argument and we solve all resulting Diophantine equations. The cases when $p = 2$ or $q = 2$ lead to no solutions in general, so we may assume that $q > 2$.

The first case is when p divides $x^2 + q^2$. Formulas (5) become

$$\begin{aligned} x &= \frac{1}{2}((u+1)^5 + (u-1)^5) = u^5 + 10u^3 + 5u; \\ q &= \frac{1}{2}((u+1)^5 - (u-1)^5) = 5u^4 + 10u^2 + 1. \end{aligned} \tag{15}$$

Since q is odd, it follows that u is even. Equation (8) leads, upon factoring it in $\mathbb{Z}[i]$ and using the fact that the only units of $\mathbb{Z}[i]$ are ± 1, $\pm i$ all of finite orders dividing 4 which is coprime to 5, to the conclusion that

$$u \pm i = (7 + 24i)(a + ib)^5 \tag{16}$$

for some integers a and b. Identifying imaginary parts above, we get

$$24a^5 + 35a^4 b - 240a^3 b^2 - 70a^2 b^3 + 120ab^4 + 7b^5 = \pm 1. \tag{17}$$

The above Thue equations (17) have no integer solutions (a, b) as confirmed by KASH [12].

We continue with the case when x is even and p divides $x^2 - q^2$. Then following through the proof of Theorem 1 we get $v = \pm 1$ and formulae (9) become

$$x = \frac{1}{2}((u+iv)^5 + (u-iv)^5) = u^5 - 10u^3 + 5u,$$
$$q = 5u^4 - 10u^2 + 1. \tag{18}$$

Equations (10) lead to

$$u^5 + 5\varepsilon u^4 - 10u^3 - 10\varepsilon u^2 + 5u + \varepsilon = y_3^5 \quad \text{for some } \varepsilon \in \{\pm 1\}. \tag{19}$$

We could either solve these equations by appealing to some general bounds from the theory of Runge's method as in [31], or we can simply argue from scratch as follows. The above equation (19) can be rewritten as

$$y_3^5 = (u+\varepsilon)^5 - 20u^3 - 20\varepsilon u^2, \tag{20}$$

therefore with $u_1 = u + \varepsilon$ we get

$$|y_3^5 - u_1^5| \le 20|u|^3 + 20|u|^2 = 20|u|^2(|u|+1).$$

If y_3 and u_1 have opposite signs, then the left–hand side above is $> |u_1|^5 \ge (|u|-1)^5$. If y_3 and u_1 have the same sign, then the left–hand side above is

$$|y_3^5 - u_1^5| \ge ||u_1| - |y_3||(|u_1|^4 + |u_1|^3|y_3| + |u_1|^2|y_3|^2 + |u_1||y_3|^3 + |y_3|^3),$$

so it is either zero or $> |u_1|^4 \ge (|u|-1)^4$. Suppose that it is zero. Then $y_3 = u_1 = u + \varepsilon$ and in equation (20) we get $20u^3 + 20u^2\varepsilon = 0$; hence, either $u = 0$, which is not allowed, or $u = -\varepsilon$, which in turn leads to $y_3 = 0$, which is not allowed either. If it is nonzero, then the above arguments show that

$$(|u|-1)^4 \le 20|u|^2(|u|+1),$$

leading to

$$|u| \le 24. \tag{21}$$

A short calculation shows that there are no solutions in this case.

We now deal with the case when x is odd and suppose that p divides $x^2 - q^2$, so $x^2 + q^2 = 2y_1^r$. The value of q from (11) is

$$q = \frac{1}{2i}((1+i)(u+iv)^5 - (1-i)(u-iv)^5)) = (u+v)(u^4 + 4u^3v - 14u^2v^2 + 4uv^3 + v^4).$$

Since q is prime, we get that either $u + v = \pm 1$, or

$$u^4 + 4u^3v - 14u^2v^2 + 4uv^3 + v^4 = \pm 1. \tag{22}$$

Equation (22) is a Thue equation which we solve with Kash. Tengely [28] also solved this equation in Section 3.II. Its only solutions are $(u, v) = \pm(2, 1)$, $\pm(1, 2)$, $(\pm 1, 0)$, $(0, \pm 1)$, which do not lead to a convenient solution to our equation (1) with $r = 5$.

So, let us assume that $u + v = \pm 1$. Let us make equations (14) explicit. Put $\alpha = u + iv$ and $\beta = u - iv$. Then

$$q = \frac{1}{2i}((1+i)\alpha^5 - (1-i)\beta^5), \quad \text{and} \quad x = \frac{1}{2}((1+i)\alpha^5 + (1-i)\beta^5).$$

Thus,

$$x + q = \frac{(1+i)}{2}\left(1 + \frac{1}{i}\right)\alpha^5 + \frac{(1-i)}{2}\left(1 - \frac{1}{i}\right)\beta^5 = \alpha^5 + \beta^5, \tag{23}$$

while

$$x - q = \frac{(1+i)}{2}\left(1 - \frac{1}{i}\right)\alpha^5 + \frac{(1-i)}{2}\left(1 + \frac{1}{i}\right)\beta^5 = i(\alpha^5 - \beta^5). \tag{24}$$

Since

$$(x+q)(x-q) = x^2 - q^2 = 2^4 p y_2^5$$

holds with some divisor y_2 of y (see (13)), and the greatest common divisor of the two factors on the left above is 2, we get, using also relations (23) and (24), that the following relations hold

$$\alpha^5 + \beta^5 = \delta y_3^5, \qquad i(\alpha^5 - \beta^5) = \delta_1 y_4^5, \tag{25}$$

where $(\delta, \delta_1) = (2, 2^3 p)$, $(2^3, 2p)$, $(2p, 2^3)$, or $(2^3 p, 2)$ and $y_3 y_4 = y_2$. Observe that by replacing (u, v, y_3, y_4) by $(v, u, -y_4, -y_3)$, which has the effect of replacing the pair (α, β) by the pair $(i\beta, -i\alpha)$, the first equation (25) above becomes the second and viceversa. Thus, we may assume that $p \mid \delta_1$. We next take a closer look at the first equation (25). It can be rewritten as

$$2u(u^4 - 10u^2v^2 + 5v^4) = \delta y_3^5, \quad \text{with } \delta \in \{2, 2^3\}.$$

Since the last factor on the left is obviously odd, the greatest common divisor of the factors $2u$ and $u^4 - 10u^2v^2 + 5v^4$ on the left is 1 or 5, and in the latter case $5 \mid u$, therefore $5 \| u^4 - 10u^2v^2 + 5v^4$, it follows that

$$u^4 - 10u^2v^2 + 5v^4 = \delta_3 y_5^5,$$
$$(\delta_3, u) \in \{(1, u_1^5), (1, 2^2u_1^5), (5, 5^4u_1^5), (5, 2^2 \cdot 5^4u_1^5)\}. \quad (26)$$

Now since $u + v = \pm 1$ it follows, up to replacing (u, v) by $(-u, -v)$, if needed (which has also the effect of changing the sign of u_1), such that $u + v = 1$, that equation (26) can also be rewritten as

$$4u^4 - 20u^2 + 20u - 5 = \delta_3 y_5^5,$$
$$(\delta_3, u) \in \{(1, u_1^5), (1, 2^2u_1^5), (5, 5^4u_1^5), (5, 2^2 \cdot 5^4u_1^5)\}. \quad (27)$$

We first treat the case when u is even since this is easier and then we deal with the case when u is odd.

Case 1. *u is even.*

The case when $u = 2^2u_1^5$ leads to

$$1024u_1^{20} - 320u_1^{10} + 80u_1^5 - 5 = y_5^5.$$

This is a Runge-type equation that can be solved by the usual steps like we did for equation (19). We found no solution.

Case 2. *u is odd.*

We look first at the instance when $u = 5^4u_1^5$. Here, $\delta = 2$, so $\delta_1 = 2^3p$. We now look at the second equation (25). Here, we get

$$v(v^4 - 10u^2v^2 + 5u^4) = \delta_1 y_4^5.$$

Since u is a multiple of 5, it follows that v is coprime to 5. If p does not divide v, then the only possibility is $v = 2^3v_1^5$, and the relation $u + v = 1$ leads to the Thue equation

$$5^4u_1^5 + 2^3v_1^5 = 1. \quad (28)$$

Reducing it modulo 5 it follows that $2^3v_1^5 \equiv 1 \pmod 5$, so $v_1 \equiv 2 \pmod 5$. Thus, $v_1^5 \equiv 2^5 \pmod{5^2}$, and reducing now equation (28) modulo 5^2 we get $2^8 \equiv 1 \pmod{5^2}$, which is false. Hence, we have no solutions in this case.

Thus, the only possibility is $p \mid v$, leading to

$$v^4 - 10u^2v^2 + 5u^4 = y_6^5,$$

which via the fact that $u + v = 1$ leads to

$$4v^4 - 20v^2 + 20v - 5 = y_6^5.$$

This all was when $u = 5^4 u_1^5$. It turns out that when $u = u_1^5$ (the remaining possibility when δ_3 is odd), one arrives at the exact same equation with the pair (v, y_6) being the pair (u, y_5) (indeed, this is just equation (27) when $\delta_3 = 1$).

Thus, it remains to deal with the equation (27) when $\delta_3 = 1$ which we write again as

$$4u^4 - 20u^2 + 20u - 5 = y_5^5. \tag{29}$$

We follow the Bilu–Hanrot method [4] together with Baker's method. We only sketch the numerical details. First, we look at the number fields generated over $\mathbb{Q}$ by some solution of the equation $4z^4 - 20z^2 + 20z - 5 = 0$. The roots z of the above equation are

$$z_1 = \frac{\sqrt{5} + \sqrt{5 - 2\sqrt{5}}}{2}, \qquad z_2 = \frac{\sqrt{5} - \sqrt{5 - 2\sqrt{5}}}{2}, \tag{30}$$

$$z_3 = \frac{-\sqrt{5} + \sqrt{5 + 2\sqrt{5}}}{2}, \qquad z_4 = \frac{-\sqrt{5} - \sqrt{5 + 2\sqrt{5}}}{2}. \tag{31}$$

We take $\alpha = z_1$ and $\beta = z_2$. Using the automorphism τ of the decomposition field of our polynomial given by

$$\tau\left(\sqrt{5 - 2\sqrt{5}}\right) = -\sqrt{5 - 2\sqrt{5}},$$

we note that $\beta = \tau(\alpha)$. Hence, we have an (α, β)-symmetry. Thus, in the notations from [4], we can work with the field $\mathbb{K}_0 = \mathbb{Q}(\alpha, \beta)^\tau = \mathbb{Q}(\alpha + \beta, \alpha\beta) = \mathbb{Q}(\sqrt{5}\,)$, instead of the entire $\mathbb{Q}(\alpha, \beta)$.

Next, we look for a complete system of admissible fields. Thus, we have to compute the finite set M in the notation from [4]. We have found that $|M| = 25$, which leads to 5 admissible fields up to isomorphism given by $\mathbb{K}_0(\mu^{1/5} + \mu^{-1/5})$, with μ in the subset M' of M given by:

$$\begin{aligned} M' = \big\{ & 480352\alpha^3 - 564608\alpha^2 - 1737872\alpha + 2042881, \\ & -149310\alpha^3 + 175518\alpha^2 + 540204\alpha - 635039, \\ & 46412\alpha^3 - 54560\alpha^2 - 167920\alpha + 197401, \\ & 4472\alpha^3 - 5248\alpha^2 - 16208\alpha + 19041, \end{aligned}$$

$$1164\alpha^3 - 1368\alpha^2 - 4212\alpha + 4951\Big\}.$$

We next computed the finite set Θ by looking for elements $\theta_0 \in \mathbb{K}$ such that

$$N_{\mathbb{K}/\mathbb{K}_0}(\theta_0)\mathcal{O}_{\mathbb{K}_0} = (\alpha - \beta)^{10}\,\mathcal{O}_{\mathbb{K}_0}.$$

We obtained a set Θ with 132 elements.

We consider the function $\varphi(w)$ given by

$$\varphi(w) = (w - \beta)\left(\zeta^k \left(\frac{w-\alpha}{w-\beta}\right)^{1/5} - 1\right)^5, \qquad w \in \mathbb{Z}, \tag{32}$$

for $k \in \{0, \ldots, 4\}$. Using Section 4.3 of [4], any integer solution (u, y_5) of equation (29) leads to an equation of the type

$$\varphi(u)^2 = \theta\eta_1^{b_1} \cdots \eta_\ell^{b_\ell}, \tag{33}$$

where $\theta \in \Theta$, and $\{\eta_1, \ldots, \eta_\ell\}$ is a system of fundamental units of $\mathbb{K}$. We put $B = \max\{|b_1|, \ldots, |b_\ell|\}$. Then we get a Baker bound for the maximal absolute value B of the exponents from equation (33) of 1.1×10^{31}. Using Section 4.6 of [4], we reduce it to 65 after three reduction steps. Finally, enumerating every possible case and testing the resulting numbers modulo every positive integer less than $X_6 = 17816$, we found after 12 hours, 11 minutes and 7 seconds that the Diophantine equation (29) has no integer solutions (u, y_5).

This completes the proof of Theorem 2. □

3. Comments

Similar remarks apply to the more general looking equation

$$x^4 - q^4 = p^s y^r, \tag{34}$$

where x and q are coprime integers, $p,\ q$ and $r \geq 5$ are primes, and $s \geq 0$. Assume first that $s = 0$. If $r \equiv 1 \pmod 4$, then the above equation has no solutions by a result from [10]. This is the case when $r = 5$. In general; i.e., even when $r \equiv 3 \pmod 4$, the above equation can have only finitely many solutions (x, q, y) by a result from [11]. Assume next that $s > 0$. Clearly, up to replacing y by $yp^{\lfloor s/r \rfloor}$, we may assume that $1 \leq s < r$. The case $s = 1$ has been treated, so let us deal with the case $s > 1$. When $p = 2$, we get that x and q are both odd, therefore

$16 \mid x^4 - q^4$. Thus, y is even if $s < 4$. This shows that up to writing $y = 2y_0$ and replacing y by y_0, and s by $s+r$, if needed, we may assume that $s \in \{4, \ldots, r+3\}$. Writing

$$x + \varepsilon q = 2^{s-2}u_1^r, \qquad x - \varepsilon q = 2u_2^r, \qquad x^2 + q^2 = 2u_3^r,$$

with integers u_1, u_2, u_3 the last two odd, we are led to the equation (4) with the exponent $2r-4$ of 2 replaced by $2(s-3)$. This has no solution by the result from [19]. Thus, we may assume that p is odd. Now one can follow through the proof of Theorem 1, and get to the conclusion that the above equation has only finitely many solutions except when

$$x = a^r + 4b^r, \quad q = |a^r - 2^{r-3}b^r|, \quad p^s c^r = a^{2r} + 2^{2r-6}b^{2r}, \quad \text{and } y = 2abc \tag{35}$$

for some integers a, b, and c. We remark that it is likely that the parametrization (35) has only finitely many solutions $(x, y, q, a, b, c, p, r, s)$ with $r \geq 5$ and $s \geq 2$. Indeed, let us look just at the equation

$$p^s c^r = a^{2r} + 2^{2r-6}b^{2r}, \tag{36}$$

and put $H = \max\{|a|, |b|\}$. Since $r > 2$ and $s \geq 2$, we get that

$$pc \leq (p^s c^r)^{1/2} < 2^r H^r.$$

Recall that the *abc*-conjecture asserts that for every $\varepsilon > 0$ there exists a positive constant C_ε such that if a, b, c are nonzero coprime integers with $a + b = c$, then

$$\max\{|a|, |b|, |c|\} \leq C_\varepsilon \mathrm{rad}(abc)^{1+\varepsilon},$$

where for a nonzero integer m we write $\mathrm{rad}(m) = \prod_{p|m} p$. Applying the *abc*-conjecture to relation (36), we get

$$H^{2r} \ll_\varepsilon (abpc)^{1+\varepsilon} \leq (2^r H^{r+2})^{1+\varepsilon},$$

therefore

$$H^{2r/(r+2)-(1+\varepsilon)} \ll_\varepsilon 1.$$

Taking $\varepsilon = 1/10$, and noticing that $2r/(r+2) = 1+(r-2)/(r+2) \geq 1+3/7$ for all $r \geq 5$, we get that $H^{23/70} \ll 1$, therefore $H \ll 1$. Note that even r was variable in the above argument. Thus, one may assume that a, b and c are fixed, and it remains in (36) to determine when the members of the linearly recurrent sequence of general term $(a^2/c)^r + (1/64)(4b^2/c)^r$ are perfect powers. There are only finitely many such instances and in practice they can be all effectively computed (see, for

example, [25]). Thus, it seems that under the *abc*-conjecture, the equation (34) should have only finitely many solutions (x, q, p, r, s) with $s \geq 2$ whenever r is fixed. Perhaps a more careful investigations of our arguments will show that in fact the *abc*-conjecture leads to the conclusion that this equation can have only finitely many solutions altogether for $r \geq 5$ (i.e., when r is a variable as well), but we did not attempt to look into this problem.

Acknowledgements. We thank Yuri Bilu, Diana Savin, Szabolcs Tengely and the anonymous referee for useful advise. Part of this work was done during very pleasant visits of F. L. and A. T. throughout 2009 and 2010, respectively, to the Mathematical Institute of the University of Bordeaux 1. Both authors thank this institute for its hospitality. During the preparation of this paper, F. L. was partly supported by an ALGANT fellowship.

References

[1] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Cambridge Philos. Soc.* **65** (1969), 439–444.

[2] P. T. Bateman and R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* **16** (1962), 363–367.

[3] Yuri Bilu, Effective analysis of integral points on algebraic curves, *Israel J. Math.* **90** (1995), 235–252.

[4] Yuri Bilu and Guillaume Hanrot, Solving superelliptic Diophantine equation by Baker's method, *Compositio Math.* **112** (1998), 273–312.

[5] Yu. Bilu, G. Hanrot and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, With an appendix by M. Mignotte, *J. Reine Angew. Math.* **539** (2001), 75–122.

[6] B. Brindza, On S-integral solutions of the equation $y^m = f(x)$, *Acta Math. Hungar.* **44**(1–2) (1984), 133–139.

[7] Y. Bugeaud, Bounds for the solutions of superelliptic equations, *Compositio Math.* **107**(2) (1997), 187–219.

[8] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll and Sz. Tengely, Integral points on hyperelliptic curves, *Algebra Number Theory* **2**(8) (2008), 859–885.

[9] J. H. E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.* **39** (1964), 537–540.

[10] H. Darmon, The equation $x^4 - y^4 = z^p$, *C.R. Math. Rep. Acad. Sci. Canada* **40** (1993), 286–290.

[11] H. Darmon and A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* **27** (1995), 513–543.

[12] M. Daberkow, C. Fieker, J. Kluners, M. E. Pohst, K. Roegner and K. Wildanger, Kant V4, *J. Symbolic Comput.* **24** (1997), 267–283.

[13] A. Grytczuk and A. Schinzel, On Runge's Theorem about Diophantine Equations, *Colloq. Math. Soc. János Bolyai* **60** (1991), 329–356.

[14] V. A. Lebesgue, Sur l'impossibilité en nombres entiers de l'equation $x^m = y^2+1$, *Nouvelle Annales des Mathématiques* (1) **9** (1850), 178–181.

[15] F. Luca, On the equation $x^2 + 2^a \cdot 3^b = y^n$, *Int. J. Math. Math. Sci.* **29** (2002), 239–244.

[16] F. Luca and A. Togbé, On the Diophantine equation $x^4 - q^4 = py^3$, *Rocky Mountain J. Math.* **40** (2010), 995–1008.

[17] PARI/GP, version `2.1.7`, *Bordeaux*, 2005, `http://pari.math.u-bordeaux.fr/`.

[18] D. Poulakis, Solutions entières de l'équation $Y^m = f(X)$, *Sém. Théor. Nombres Bordeaux* (2) **3**(1) (1991), 187–219.

[19] K. Ribet, On the equation $a^p + 2^\alpha b^p + c^p = 0$, *Acta Arith.* **79** (1997), 7–16.

[20] C. Runge, Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen, *J. Reine Angew. Math.* **100** (1887), 425–435.

[21] A. Sankaranarayanan and N. Saradha, Estimates for the solutions of certain Diophantine equations by Runge's method, *Int. J. Number Theory* **4**(3) (2008), 475–493.

[22] D. Savin, On the Diophantine equation $x^4 - q^4 = py^5$, *Ital. J. Pure Appl. Math.* **26** (2009), 103–108.

[23] A. Schinzel and W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958), 185–208, Corrigendum, ibid. **5** (1960), 259.

[24] W. M. Schmidt, Integer points on curves of genus 1, *Compositio Math.* **81**(1) (1992), 33–59.

[25] T. N. Shorey and R. Tijdeman, Exponential Diophantine equations, Vol. 87, Cambridge Tracts in Mathematics, *Cambridge University Press, Cambridge*, 1986.

[26] V. G. Sprindžuk, The arithmetic structure of integer polynomials and class numbers, *Trudy Mat. Inst. Steklov.* **143** (1977), 152–174.

[27] Sz. Tengely, On the Diophantine equation $F(x) = G(y)$, *Acta Arithmetica* **110** (2003), 185–200.

[28] Sz. Tengely, On the Diophantine equation $x^2 + a^2 = 2y^p$, *Indag. Math. New Series* **15** (2004), 291–304.

[29] Sz. Tengely, On the Diophantine equation $x^2 + q^{2m} = 2y^p$, *Acta Arithmetica* **127** (2007), 71–86.

[30] P. M. Voutier, An upper bound for the size of integral solutions to $Y^m = f(X)$, *J. Number Theory* **53**(2) (1995), 247–271.

[31] P. G. Walsh, A quantitative version of Runge's theorem on Diophantine equations, *Acta Arith.* **62** (1992), 157–172, Correction to: A quantitative version of Runge's theorem on Diophantine equations, *Acta Arith.* **73** (1995), 397–398.

AURÉLIEN BAJOLET
UNIVERSITÉ DE BORDEAUX 1
INSTITUT DE MATHÉMATIQUES
351 COURS DE LA LIBÉRATION
33404 TALENCE
FRANCE
E-mail: aurelien.bajolet@math.u-bordeaux1.fr

BENJAMIN DUPUY
UNIVERSITÉ DE BORDEAUX 1
INSTITUT DE MATHÉMATIQUES
351 COURS DE LA LIBÉRATION
33404 TALENCE
FRANCE
E-mail: benjamin.dupuy@math.u-bordeaux1.fr

FLORIAN LUCA
CENTRO DE CIENCIAS
MATEMÁTICAS
UNIVERSIDAD NACIONAL
AUTÓNOMA DE MÉXICO
C.P. 58089, MORELIA
MICHOACÁN
MÉXICO
E-mail: fluca@matmor.unam.mx

ALAIN TOGBÉ
MATHEMATICS DEPARTMENT
PURDUE UNIVERSITY
NORTH CENTRAL
1401 S, U.S. 421
WESTVILLE IN 46391
USA
E-mail: atogbe@pnc.edu

(Received November 8, 2010; revised October 8, 2011)