ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 40, Number 3, 2010

ON THE DIOPHANTINE EQUATION $x^4 - q^4 = py^3$

FLORIAN LUCA AND ALAIN TOGBÉ

ABSTRACT. In this paper, we improve upon some recent results of Savin [**11**] on the Diophantine equation from the title.

1. Introduction. In [**11**], Savin showed that the Diophantine equation

$$x^4 - q^4 = py^3 \tag{1}$$

has no solutions in integers x, y, p, q subject to the following restrictions:

(i) p and q are distinct primes;

(ii) p does not divide x;

(iii) $p \equiv 11 \pmod{12}$ and $q \equiv 1 \pmod{3}$;

(iv) p is a primitive root modulo q;

(v) 2 is a cubic residue modulo q.

Note, however, that equation (1) has the solution $x = \pm q$ and $y = 0$, so the condition $y \neq 0$ should be imposed.

In this paper, we relax most of Savin's restrictions. Our first result is:

Theorem 1. *The Diophantine equation* (1) *has no integer solutions* (x, y, p, q) *with* $\gcd(x, y) = 1$, $xy \neq 0$, *and* p *and* q *primes.*

One may ask what happens if we do not impose the restriction that x and y are coprime. Well, then there must be a prime $r \mid \gcd(x, y)$.

2010 AMS *Mathematics subject classification.* Primary 54B20, 54F15.
The first author was partially supported by grants SEP-CONACyT 46755 and PAPIIT 100508. The second author was partially supported by Purdue University North Central.
Received by the editors on December 10, 2007, and in revised form on December 30, 2007.
DOI:10.1216/RMJ-2010-40-3-995

Clearly, this prime must divide q^4, so it is in fact q. Writing $x = qx_0$, we get $q^4(x_0^4 - 1) = py^3$, and since $p \neq q$, we get that $y = q^2 y_0$ and later that $x_0^4 - 1 = pq^2 y_0^3$. Concerning this equation, we have not been able to prove any finiteness result of the same generality as Theorem 1. However, we can show that this equation does not have any solutions under Savin's restrictions (iii)–(v). We record this as follows:

Theorem 2. *The Diophantine equation*

$$x^4 - 1 = pq^2 y^3 \tag{2}$$

has no integer solutions (x, y, p, q) *with* $y \neq 0$, *and* p *and* q *primes satisfying the conditions* (iii)–(v) *above.*

We suspect that equation (2) has only finitely many integer solutions. We record this suspicion as:

Conjecture 1. *Equation* (2) *has only finitely many positive integer solutions* (x, y, p, q) *with* p *and* q *prime numbers.*

In the last section of the paper, we give heuristics supporting Conjecture 1.

2. Preliminary considerations. We shall assume that x, y, p, q are integers with p and q primes and $y \neq 0$. Clearly, we may assume that $x \geq 0$. The sign of y is then determined by the sign of $x^4 - q^4$. The case when $p = q$ can be handled easily by the following argument. If $p = q$, then p divides two of the three terms involved in (1), so it must divide the remaining one x^4. Thus, $x = px_0$ leading to $p^4(x_0^4 - 1) = py^3$. The above equation implies that $p \mid y$ and, with $y = py_0$, we get $x_0^4 - 1 = y_0^3$, which has the uninteresting solutions $(x_0, y_0) = (0, -1), (\pm 1, 0)$. From now on, we assume that $x_0 y_0 > 0$. Then our equation is a particular case of Catalan's equation $x^n - y^m = 1$ in positive integer variables x, y, m, n all > 1 which was recently completely solved by Mihăilescu [**10**]. However, the instance relevant to us, namely the case $n = 4$, follows from Ko's work [**2**], who showed more than 40 years ago that the only positive solution of the equation $x^2 - 1 = y^m$ with $m > 1$ is

$x = 3$, $y = 2$, $m = 3$. Since 3 is not a perfect square, it follows that $x_0^4 - 1 = y_0^3$ does not have any positive integer solutions (x_0, y_0).

From now on, we shall assume that $p \neq q$ and that $x \geq 0$. In particular, $x > 0$. We now comment on the case $q = 2$.

If x is odd, then the left-hand side of equation (1) factors as $(x^2 - 4)(x^2 + 4)$ and these two factors are coprime. Thus, either $x^2 - 4 = u^3$ or $x^2 + 4 = u^3$ holds with some divisor u of y.

The curve $X^2 = U^3 + 4$ is elliptic and appears as curve 108A1 of Cremona's tables available online free of charge at [**4**]. It has rank 0 and torsion group of order 3 formed by the points $(X, U) = (\pm 2, 0)$ together with the point at infinity. Thus, the first of the two equations above does not lead to any solutions. The second one corresponds to the elliptic curve $X^2 = U^3 - 4$, which is curve 432B1. This has trivial torsion and rank 1 with $(X, U) = (2, 2)$ as the generator. However, Luca [**9**] has determined all solutions of the equation $x^2 + 2^a \cdot 3^b = y^n$ with integers $a \geq 0$, $b \geq 0$, $n \geq 3$ and x and y coprime. A quick investigation of his list reveals that $(x, u) = (11, 5)$ is the only solution of the equation $x^2 + 4 = u^3$ with x odd. For this solution, $x^2 - 4 = 121 - 4 = 117 = 3^2 \cdot 13$ is not of the form pv^3 for some prime p and integer v. So, there is no solution in this case either.

If x is even, then $x = 2x_0$. In this case, $16 \mid py^3$, therefore $4 \mid y$. With $y = 4y_0$, we get the equation $x_0^4 - 1 = 4py_0^3$. Hence, x_0 is odd, so $2 \| x_0^2 + 1$. It now follows that there exists a divisor u of y_0 such that either $x_0^2 - 1 = 2u^3$ or $x_0^2 + 1 = 2u^3$. The first Diophantine equation leads to $(2x_0)^2 = (2u)^3 + 4$, a particular integer solution $(X, U) = (2x_0, 2u_0)$ of the Diophantine equation $X^2 = U^3 + 4$ with $U = u \neq 0$, which, by the above remarks, does not exist because the curve 108A1 does not have a rational point (x, u) with $u \neq 0$. The second Diophantine equation $x_0^2 - 2u^3 = -1$ was treated a long time ago by Cohn in [**3**] (in fact, he treated the more general Diophantine equation $x^2 - 2u^m = -1$ with $m > 2$ except for $m = 4$, which had been treated much earlier by Ljunggren [**8**]), who showed that its only integer solution (x_0, u) is $(x_0, u) = (0, 1)$. However, this leads to $x = 0$, which we are excluding.

From now on, we shall assume that $x > 0$, that $p \neq q$, and that q is odd.

2.1. The proof of Theorem 1. Since x and y are coprime, we deduce easily that q does not divide x (otherwise, q^4 divides py^3; therefore, q divides both x and y, which is a contradiction). We write the left-hand side of equation (1) as $(x^2-q^2)(x^2+q^2)$. At this stage, the proof splits naturally into two cases.

The easy case. $p \nmid x^2+q^2$. Note that this is the case say when $p \equiv 3 \pmod 4$, since such primes cannot divide a sum of two coprime squares. In this case, p will divide one of $x-q$ and $x+q$.

If x is odd, then $2 \| x^2+q^2$. Further, one of $x-q$ and $x+q$ is congruent to 2 modulo 4 and the other one is also even. From this analysis and unique factorization, it follows easily that the relations $x+\eta q = 2u^3$ and $x^2+q^2 = 2v^3$ hold with some divisors u and v of y and some $\eta \in \{\pm 1\}$. Multiplying these two relations we get $(x+\eta q)(x^2+q^2) = 4(uv)^3$. With $X := \eta x/q$ and $Y := \eta uv/q$, we get the Diophantine equation $(X+1)(X^2+1) = 4Y^3$ in rational numbers X and Y. Straightforward algebraic manipulations show that this equation can be rewritten as

$$\left(\frac{2}{X+1} - 1\right)^2 = \left(\frac{2Y}{X+1}\right)^3 - 1.$$

Thus, with $U := 2/(X+1) - 1$ and $V := 2Y/(X+1)$, we get that our equation is birationally equivalent to

$$U^2 = V^3 - 1.$$

This elliptic curve is curve 144A1 in Cremona's table which has rank 0 and torsion group consisting of only two points, namely $(U,V) = (0,1)$, and the point at infinity. These correspond to $X = \pm 1$, so $x = \pm q$ and $y = 0$, and such solutions are not convenient for us.

If x is even, then $x-q$, $x+q$ and x^2+q^2 are coprime any two, so we deduce that the relations $x+\eta q = u^3$ and $x^2+q^2 = v^3$ hold with some divisors u and v of y and some $\eta \in \{\pm 1\}$. The same argument as above leads to the Diophantine equation $U^2 = V^3 - 4$ with $U := 4/(X+1) - 2$, $V := 2Y/(X+1)$, where again $X := \eta x/q$, $Y := \eta uv/q$, but this elliptic curve is 432B1 and has rank 1; in particular, infinitely many rational points on it.

So, we continue by invoking a divisibility argument in $\mathbf{Z}[i]$. Write $x^2+q^2 = (x+iq)(x-iq)$. Since x and q are coprime, x is even and

q is odd, one checks easily that $x + iq$ and $x - iq$ are coprime in $\mathbf{Z}[i]$. Since their product is a cube, each one is associated to a cube. Since the only units of $\mathbf{Z}[i]$ are ± 1, $\pm i$ of orders dividing 4, which is coprime to 3, it follows that we may assume that an issue about units does not occur so $x + iq = (a + ib)^3$. Identifying real and imaginary parts in this last relation, we get that $x = a^3 - 3ab^2$ and $q = b(3a^2 - b^2)$. Since q is prime, we get that either $b = \pm 1$, or $3a^2 - b^2 = \pm 1$.

We first treat the case $b = \pm 1$. Then $q = \mp(3a^2 - 1)$. Since $q > 1$, we get that $q = 3a^2 - 1$; thus, $b = 1$. Hence, $x = a^3 - 3a$. Then

$$x + \eta q = a^3 - 3a + \eta(3a^2 - 1) = \eta(a_1^3 + 3a_1^2 - 3a_1 - 1),$$

where $a_1 := \eta a$. Writing $u_1 := \eta u$, we get that

$$a_1^3 + 3a_1^2 - 3a_1 - 1 = \eta(x + q) = \eta u^3 = u_1^3.$$

Thus,

$$(a_1 + 1)^3 - 6a_1 - 2 = u_1^3.$$

Considerations modulo 2 show that $u_1 \equiv a_1 + 1 \pmod 2$. Certainly, $u_1 \neq a_1 + 1$ because this would lead to $a_1 = -1/3$, which is impossible. Thus, $|u_1 - (a_1 + 1)| \geq 2$. In particular,

$$\begin{aligned} |6a_1 + 2| &= |u_1^3 - (a_1 + 1)^3| \\ &= |u_1 - (a_1 + 1)||u_1^2 + u_1(a_1 + 1) + (a_1 + 1)^2| \\ &= |u_1 - (a_1 + 1)||(u_1 + (a_1 + 1)/2)^2 + 3(a_1 + 1)^2/4| \\ &\geq \frac{3}{2}(a_1 + 1)^2. \end{aligned}$$

Writing $z := |a_1 + 1|$, we have

$$\frac{3z^2}{2} \leq |6(a_1 + 1) - 4| \leq 6z + 4,$$

which leads to $z \leq 4$; therefore, $a_1 \in \{-5, -4, \ldots, 3\}$. A quick check reveals that the only acceptable values are $a_1 = -3$, $u_1 = 2$ and $a_1 = 1$, $u_1 = 0$, none of which is convenient since our value for y is odd (because x is even and q is odd), so it cannot have an even divisor u.

In the second case, we have that $3a^2 - b^2 = \pm 1$. The case of the sign $+$ is impossible by considerations modulo 3 because -1 is not a quadratic

residue modulo 3. Thus, $3a^2 - b^2 = -1$, and since $q = b(3a^2 - b^2)$, we must have that $b = -q$. This leads to $q^2 - 3a^2 = 1$, so $q = \sqrt{3a^2+1}$. Now $x = a^3 - 3ab^2 = a^3 - 3a(3a^2+1) = -8a^3 - 3a$. Thus,

$$u^3 = x + \eta q = -8a^3 - 3a \pm \sqrt{3a^2+1},$$

leading to

$$\begin{aligned} |3a \pm \sqrt{3a^2+1}| &= |u^3 + 8a^3| \\ &= |u+2a||u^2 - 2ua + 4a^2| \\ &= |u+2a||(u-a)^2 + 3a^2| \\ &\geq 3a^2. \end{aligned}$$

In the above, we used the fact that $u + 2a \neq 0$ (because u is odd), so $|u+2a| \geq 1$. Thus,

$$3a^2 \leq |3a \pm \sqrt{3a^2+1}| \leq 5|a|,$$

so $|a| < 2$, giving $a \in \{\pm 1, 0\}$. However, none of these values for a gives an odd prime value for q in the relation $q^2 = 3a^2 + 1$.

This completes the argument for the easy case.

The hard case. $p \mid x^2 + q^2$. In this case, $x^2 + q^2 = p\delta u^3$, where $\delta = 1$ or 2 according to whether x is even or odd. Further, $x - q = \delta v^3$ and $x + q = \delta w^3$. Here, u, v and w are integers such that $y = \delta uvw$. From the above equations, we get that

$$q = \frac{\delta}{2}(w^3 - v^3) = \frac{\delta}{2}(w-v)(w^2 + wv + v^2).$$

Furthermore, since x and q are positive, it follows that u and w are positive and $w > v$. Moreover, $w \geq ((x+q)/2)^{1/3} \geq ((1+3)/2)^{1/3} = 2^{1/3} > 1$, so $w \geq 2$. Thus, $w^2 + vw + v^2 = (v + w/2)^2 + 3w^2/4 \geq 3$. Since q is prime, we conclude that $w - v = 1$ if $\delta = 2$. If $\delta = 1$, then since $w^2 + vw + v^2 \geq 3$ is odd, we must have $w - v = 2$. Thus,

$$\begin{aligned} q &= (v+1)^3 - v^3 = 3v^2 + 3v + 1; \\ x &= (v+1)^3 + v^3 = 2v^3 + 3v^2 + 3v + 1, \end{aligned} \tag{3}$$

when $\delta = 2$, and

$$\begin{aligned} q &= \frac{(v+2)^3 - v^3}{2} = 3v^2 + 6v + 4, \\ x &= \frac{(v+2)^3 + v^3}{2} = v^3 + 3v^2 + 6v + 4, \end{aligned} \tag{4}$$

when $\delta = 1$.

Let us first treat the case $\delta = 2$. In this case

$$x^2 + q^2 = ((v+1)^3 + v^3)^2 + ((v+1)^3 - v^3)^2 = 2((v+1)^6 + v^6),$$

therefore

$$(v+1)^6 + v^6 = pu^3.$$

Note that the left-hand side above factors as

$$(v+1)^6 + v^6 = ((v+1)^2 + v^2)((v+1)^4 - v^2(v+1)^2 + v^4). \tag{5}$$

Furthermore, the two factors above are coprime, since if r is a prime dividing both of them, we then get that $(v+1)^2 \equiv -v^2 \pmod{r}$; therefore,

$$(v+1)^4 - v^2(v+1)^2 + v^4 \equiv v^4 + v^4 + v^4 \pmod{r} \equiv 3v^4 \pmod{r}.$$

Since in fact r divides the left-hand side of the above congruence, but not v (otherwise it will also divide $v+1$, which is impossible), we get that $r \mid 3$; so, $r = 3$. However, 3 cannot divide the number $(v+1)^6 + v^6$ which is a sum of two coprime squares. Since the two factors appearing in the righthand side of the formula (5) are coprime and their product is p times a cube, we get, by unique factorization, then either the first factor or the second factor is a cube. In case the first factor is a cube, we get $(v+1)^2 + v^2 = t^3$; therefore, $2v^2 + 2v + 1 = t^3$ or $(2v+1)^2 + 1 = 2t^3$. By Cohn's result from [**3**] mentioned previously, the only solutions are $v = -1, 0$ and $t = 1$, giving $q = 1$, which is not prime. Thus, we conclude that p divides the first factor in (5), so

$$(v+1)^4 - v^2(v+1)^2 + v^4 = s^3 \tag{6}$$

holds with some integer s. This equation can be rewritten as

$$(v^2 + v + 2)^2 = s^3 + 3. \tag{7}$$

With $Y = v^2+v+2$ and $X = s$, we have the elliptic curve $Y^2 = X^3+3$. MAGMA (see [**1**]) found that the only integer point on the above elliptic curve is $(X, Y) = (1, 2)$, for which $v = 0$ or -2. None of these produces any convenient solution (x, y, p, q) of our original Diophantine equation (1).

We now return to the instance when $\delta = 1$. In this case, formulas (4) give us

$$\begin{aligned} pu^3 = x^2 + q^2 &= \left(\frac{(v+2)^3 + v^3}{2}\right)^2 + \left(\frac{(v+2)^3 - v^3}{2}\right)^2 \\ &= \frac{(v+2)^6 + v^6}{2} \\ &= \left(\frac{(v+2)^2 + v^2}{2}\right)((v+2)^4 - (v+2)^2v^2 + v^4). \end{aligned} \tag{8}$$

The previous analysis shows that the two factors appearing in the righthand side above are coprime. If p does not divide the smaller one, then this factor must be a cube. Certainly, this is also $v^2 + 2v + 2 = (v+1)^2+1$ and this cannot be a cube by a very old result of Lebesgue [**7**]. Hence, the prime p divides the smaller factor and we get that

$$(v+2)^4 - v^2(v+2)^2 + v^4 = s^3 \tag{9}$$

holds with some positive integer s. This last equation can be rewritten as

$$(v^2 + 2v + 8)^2 = s^3 + 48. \tag{10}$$

Putting $Y = v^2 + 2v + 8$ and $X = s$ we get the elliptic curve $Y^2 = X^3 + 48$. MAGMA [**1**] found that its only integer point is $(X, Y) = (1, 7)$, leading to $v = -1$, which does not produce a convenient solution (x, y, p, q) of our Diophantine equation (1).

This completes the proof of Theorem 1. □

3. The proof of Theorem 2. Again, we can assume that $p \neq q$, that $x > 0$, and that q is odd since the other cases have been treated in Section 2. The righthand side of equation (2) then factors as $(x-1)(x+1)(x^2+1)$. Since $p \not\equiv 1 \pmod 4$, it follows that p cannot

divide the last factor. If q does not divide the last factor, then either $x^2+1 = u^3$ or $x^2+1 = 2u^3$ must hold with some divisor u of y, and these are impossible by the results of Lebesgue and Cohn, respectively. So, $q \mid x^2+1$. It is clear that either $x-1$, $x+1$ and x^2+1 are mutually coprime or they are all even but $2 \| x^2+1$ and one of $x-1$ and $x+1$ is congruent to 2 modulo 4. Thus, $x^2+1 = \delta q^2 u^3$, $x - \eta = \delta v^3$ and $x + \eta = \delta p w^3$, where $\delta \in \{1,2\}$ and $\eta \in \{\pm 1\}$. From the last two relations, we get $2\eta = \delta(pw^3 - v^3)$. We write $v_1 := \eta v$, $w_1 := \eta w$ and $x_1 := \eta x$. Thus, $2 = \delta(pw_1^3 - v_1^3)$.

Assume that $\delta = 2$. Then $1 = pw_1^3 - v_1^3$; therefore, $pw_1^3 = v_1^3 + 1 = (v_1+1)(v_1^2 - v_1 + 1)$. The congruence $X^2 - X + 1 \equiv 0 \pmod{p}$ when p is odd is equivalent to $(2X-1)^2 \equiv -3 \pmod{p}$, and this has a solution modulo p if and only if -3 is a quadratic residue modulo p. By quadratic reciprocity, this happens if and only if $p \equiv 1 \pmod{3}$. But our prime p is not congruent to $1 \pmod{3}$. Thus, p cannot divide $v_1^2 - v_1 + 1$. Furthermore, one can easily check that the only prime r that might divide both $v_1 + 1$ and $v_1^2 - v_1 + 1$ is $r = 3$, and if this actually happens then $3 \| v_1^2 - v_1 + 1$. Armed with these facts, the above Diophantine equation $pw_1^3 = (v_1+1)(v_1^2 - v_1 + 1)$ leads to either $v_1^2 - v_1 + 1 = t^3$ or $v_1^2 - v_1 + 1 = 3t^3$ for some positive integer t, where for the first equation $3 \nmid t$. The first equation can be regrouped as

$$(2v_1 - 1)^2 + 3 = 4t^3.$$

Thus, with $z_1 := 2v_1 - 1$, we get

$$\left(\frac{z_1 + i\sqrt{3}}{2}\right)\left(\frac{z_1 - i\sqrt{3}}{2}\right) = t^3,$$

and the two factors above are coprime in $\mathbf{Z}[(1+i\sqrt{3})/2]$, which is Euclidean. The only units of this ring are $\pm\omega^c$, where ω is a primitive root of unity of order 3 and $c \in \{0,1,2\}$. Thus, we get that there exist $c \in \{0,1,2\}$ and integers a and b of the same parity such that

$$\frac{z_1 + i\sqrt{3}}{2} = \omega^c \left(\frac{a + i\sqrt{3}b}{2}\right)^3.$$

Taking $\omega = (-1 + i\sqrt{3})/2$, and $c = 0, 1, 2$, and identifying imaginary parts from both sides of the above equation, we get the Thue equations

$$\begin{aligned} 4 &= 3a^2b - 3b^3 && (c = 0);\\ 8 &= a^3 - 3a^2b - 9ab^2 + 3b^3 && (c = 1);\\ 8 &= -a^3 - 3a^2b + 9ab^2 + 3b^3 && (c = 2). \end{aligned}$$

We used Kash [**5**] to compute all the solutions of each of these three Diophantine equations. None of these solutions leads to any convenient solution (x, y, p, q) of our Diophantine equation (2), although some of them gave us an interesting near miss. Namely, $(a, b) = (5, 1)$ is a solution to the above Thue equation when $c = -1$. This leads to $t = 7$, so $v_1^2 - v_1 + 1 = 7^3$ giving $v_1 = -18, 19$. The case when $v_1 = -18$ gives $\eta = -1$, $p = 17$, $w = 7$ and $x = 11663$. However, $(x^2 + 1)/2 = 68012785 = 5 \cdot 13602557$ is a product of two primes and so is not of the form q^2u^3 for some prime q and integer u. The case $v_1 = 19$ gives $v_1^3 + 1 = 2^2 \cdot 5 \cdot 7^3$ which is not of the form pw_1^3 for some prime p and integer w_1.

The case when $v_1^2 - v_1 + 1 = 3t^2$ can be dealt with analogously. Namely, here we note that the equation can be rewritten as $(2v_1 - 1)^2 + 3 = 12t^2$. Thus, $3 \mid 2v_1 - 1$. Writing $z_1 := (2v_1 - 1)/3$, we get $3z_1^2 + 1 = 4t^3$, which can be rewritten as

$$\left(\frac{1 + i\sqrt{3}z_1}{2}\right)\left(\frac{1 - i\sqrt{3}z_1}{2}\right) = t^3.$$

The two numbers appearing above are coprime in $\mathbf{Z}[(1 + i\sqrt{3})/2]$, so we get again an equation of the form

$$\frac{1 + i\sqrt{3}z_1}{2} = \omega^c\left(\frac{a + i\sqrt{3}b}{2}\right)^3$$

with $c \in \{0, 1, 2\}$ and a and b integers of the same parity. Writing again $\omega = (-1 + i\sqrt{3})/2$ and identifying real parts, we are led again to three Thue equations, which we solved with Kash [**5**]. None of the resulting solutions (a, b, c) leads to any solution (x, y, p, q) of our initial equation (2).

We now assume that $\delta = 1$. Then $x_1 = pw_1^3 - 1$ and $x_1 = v_1^3 + 1$. Thus, $pw_1^3 = v_1^3 + 2$. Now $q^2u^3 = x_1^2 + 1 = (pw_1^3 - 1)^2 + 1 = pw_1^3(pw_1^3 - 2) + 2 = p(v_1w_1)^3 + 2$. Thus, $q^2u^3 = p(v_1w_1)^3 + 2$. This shows that $p2^{-1}$ is a cubic residue modulo q (note that $q \equiv 1 \pmod 3$, so it makes sense to talk about cubic residues modulo q). Since 2 is a cubic residue modulo q, so is p. This contradicts the fact that p was a primitive root modulo q. Note that in fact from condition (v) the only information that we used is the fact that p is not a cubic residue modulo q, and not the full information that p is a primitive root modulo q.

4. Heuristics on equation (2). Here, we give heuristics which seem to support Conjecture 1. Throughout this section, we use the Vinogradov symbols $\gg$ and $\ll$ and the Landau symbol O with their usual meanings. Recall that if f and g are functions, then $f \ll g$ and $f = O(g)$ are both equivalent to the fact that there exists a constant K such that the inequality $|f(x)| < Kg(x)$ holds for all sufficiently large values of x, and $g \gg f$ is equivalent to $f \ll g$. If the constants implied by the above symbols depend on other parameters like λ or μ, we shall write $f \ll_\lambda g$ or $f = O_\mu(g)$ to indicate such a dependence. For a nonzero integer m, let $N(m) := \prod_{p|m} p$ be the algebraic radical of m. We start by recalling the ABC conjecture formulated by Masser and Oesterlé in 1985.

Conjecture 2. *For all $\varepsilon > 0$ the inequality*

$$\max\{|A|, |B|, |C|\} \ll_\varepsilon N(ABC)^{1+\varepsilon}$$

holds for all triples of coprime nonzero integers A, B, C with $A+B = C$.

Elkies [**6**] used a theorem of Belyi to deduce that the above ABC conjecture 2 implies the following more general version of itself.

Conjecture 3. *Let $f(X, Y)$ be a homogeneous form of degree $d > 1$ with integer coefficients without repeated factors over $\mathcal{C}[X, Y]$. Then the ABC conjecture implies that for every ε, the inequality*

$$|N(f(m, n))| \gg_{\varepsilon, f} (\max\{m, n\})^{d-2-\varepsilon}$$

holds.

Of course, the ABC conjecture 2 is just the above statement for the form $f(X, Y) = XY(X + Y)$.

We now start our arguments. We assume as before that $xy > 0$, that $p \neq q$ and that q is odd. The left-hand side of equation (2) factors as $(x^2 - 1)(x^2 + 1)$. We distinguish the following cases.

Case 1. Both p and q^2 divide the same factor $x^2 + \eta$ for some $\eta \in \{\pm 1\}$.

In this case, since $\gcd(x^2-1, x^2+1)$ is either 1 or 2 it follows, by unique factorization, that $x^2 - \eta = \delta u^3$ for some $\delta \in \{1, 2, 4\}$ and some positive integer u. But such Diophantine equations have only finitely many positive integer solutions (x, u).

From now on, we assume that p divides one of the factors $x^2 \pm 1$ and q^2 divides the other factor.

Case 2. q^2 divides $x^2 - 1$.

In this case we get, again by unique factorization and the fact that $\gcd(x^2-1, x^2+1)$ is either 1 or 2, that $x^2 - 1 = \delta q^2 u^3$ for some positive integer u and some $\delta \in \{1, 2, 4\}$. We apply the ABC Conjecture 2 to the above equation to deduce that for any fixed $\varepsilon > 0$ we have

$$x^{2(1-\varepsilon)} \ll_\varepsilon N(\delta x^2 q w^3) \ll_\varepsilon x\, qw.$$

Since $q^2 w^3 < x^2$, we get that $w < x^{2/3}/q^{2/3}$. Thus, we get

$$x^{2(1-\varepsilon)} \ll_\varepsilon xqx^{2/3}/q^{2/3} \ll_\varepsilon x^{5/3} q^{1/3},$$

leading to $q \gg_\varepsilon x^{1-6\varepsilon}$. Choosing $\varepsilon := 1/20$, we get that $q \gg x^{2/3}$. Thus, $q^2 \gg x^{4/3}$. But q^2 divides $x^2 - 1 = (x-1)(x+1)$ and the greatest common divisor of $(x-1)$ and $(x+1)$ is at most 2. Thus, q^2 divides one of $x \pm 1$, leading to $x \pm 1 \geq q^2 \gg x^{4/3}$. Hence, $x = O(1)$ in this case also.

Case 3. q^2 divides $x^2 + 1$.

Then $p \mid (x^2-1) = (x+1)(x-1)$. In this case we get, again by unique factorization, that there exists $\delta \in \{1, 2\}$, $\eta \in \{\pm 1\}$ and divisors u and v of y such that $x^2+1 = \delta q^2 u^3$ and $x+\eta = \delta v^3$. Let $x_1 := \eta x$, $u_1 := \eta u$ and $v_1 := \eta v$. Let $f(X, Y) := (X - Y)(2X - Y)(X^2 + (X - Y)^2)$. It is easy to see that $f(X, Y)$ is a form of degree $d = 4$ without repeated factors. Note that

$$f(x_1, x_1 - 1) = (x_1 + 1)(x_1^2 + 1) = \eta \delta^2 q^2 u^3 v^3;$$

therefore,

$$N(f(x_1, x_1 - 1)) \leq 2\, quv.$$

Since $v \leq (|x_1|+1)^{1/3}$ and $u \leq ((x_1^2+1)/q^2)^{1/3}$, we get that

$$N(f(x_1, x_1-1)) \ll quv \ll q|x_1|^{1/3}(|x_1|^2/q^2)^{1/3} = q^{1/3}|x_1|.$$

However, Conjecture 3 implies that if $|x_1| > 1$, then $N(f(x_1, x_1-1)) \gg_\varepsilon |x_1|^{2-\varepsilon}$. Combining these inequalities, we get that $q^{1/3} \gg_\varepsilon |x_1|^{1-\varepsilon}$, so $q \gg_\varepsilon |x_1|^{3(1-\varepsilon)}$. However, since $x^2+1 = \delta q^2 u^3$, we certainly have that $q^2 \leq x^2+1 \leq 2|x_1|^2$. Thus, $|x_1|^{3(1-\varepsilon)} \ll_\varepsilon q \ll |x_1|$. Choosing $\varepsilon = 1/2$, we get that $x = |x_1| = O(1)$.

To summarize, we infer that only finitely many positive integer solutions (x, p, q, y) of the Diophantine equation (2) are possible under the ABC Conjecture.

Acknowledgments. We thank the referee for useful suggestions and for observing that Diophantine equations (6) and (9) can be rewritten as (7) and (10), respectively. These observations shortened our original proof of Theorem 1 which was considerably longer. This paper was written during Spring 2007 when F.L. visited the Williams College. He thanks the Mathematics Department there for its hospitality during his visit.

REFERENCES

1. Wieb Bosma, John Cannon and Catherine Playoust, *The Magma algebra system*. I. *The user language*, J. Symbolic Comput. **24** (1997), 235–265.

2. K. Chao, *On the diophantine equation* $x^2 = y^n + 1$, $xy \neq 0$, Sci. Sinica (Notes) **14** (1964), 457–460.

3. J.H.E. Cohn, *Perfect Pell powers*, Glasgow Math. J. **38** (1996), 19–20.

4. J.E. Cremona, *Elliptic curve data*, http://www.maths.nott.ac.uk/personal/jec/ftp/data.

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

6. N.D. Elkies, *abc implies Mordell*, Int. Math. Res. Not. **1991** (1991), 99–109.

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

8. W. Ljunggren, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$, Avh. Norske Vid. Akad. Oslo. I. **1942** (1942), 27 pages.

9. F. Luca, *On the equation is* $x^2 + 2^a 3^b = y^n$, Internat. J. Math. Math. Sci. **29** (2002), 239–244.

10. P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. reine Angew. Math. **572** (2004), 167–195.

11. D. Savin, *On the diophantine equation* $x^4 - q^4 = py^3$, An. Şt. Univ. Ovidius Constanţa **12** (2004), 81–90.

Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México
Email address: fluca@matmor.unam.mx

Mathematics Department, Purdue University, North Central 1401 S, U.S. 421, Westville IN 46391
Email address: atogbe@pnc.edu