



On $px^2 + q^{2n} = y^p$ and related Diophantine equations

A. Laradji^a, M. Mignotte^b, N. Tzanakis^{c,*}

^a Department of Mathematics & Statistics, KFUPM, Dhahran, Saudi Arabia

^b Université Louis Pasteur, U. F. R. de Mathématiques, Strasbourg, France

^c Department of Mathematics, University of Crete, Iraklion, Greece

ARTICLE INFO

Article history:

Received 2 February 2010

Accepted 28 February 2011

Available online 15 April 2011

Communicated by Michael A. Bennett

Keywords:

Exponential Diophantine equation

Linear forms in two logarithms

Hypergeometric series

Lehmer pair

Cyclotomic polynomial

ABSTRACT

The title equation, where $p > 3$ is a prime number $\not\equiv 7 \pmod{8}$, q is an odd prime number and x, y, n are positive integers with x, y relatively prime, is studied. When $p \equiv 3 \pmod{8}$, we prove (Theorem 2.3) that there are no solutions. For $p \not\equiv 3 \pmod{8}$ the treatment of the equation turns out to be a difficult task. We focus our attention to $p = 5$, by reason of an article by F. Abu Muriefah, published in J. Number Theory 128 (2008) 1670–1675. Our main result concerning this special equation is Theorem 1.1, whose proof is based on results around the Diophantine equation $5x^2 - 4 = y^n$ (integer solutions), interesting in themselves, which are exposed in Sections 3 and 4. These last results are obtained by using tools such as linear forms in two logarithms and hypergeometric series.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

Diophantine equations of the form $px^2 + c = y^p$, where c is a non-zero integer and p is an odd prime, have been studied by several authors. When $c = 2^n$, the case $p = 3$ was solved by Rabinowitz in [27], while Le dealt with the case $p > 3$ in [24]. The case $c = 3^n$ was considered by Abu Muriefah in [2]. Cao [17] treated the cases $c = 1$ and $c = 4^n$ (see also [1,5,11,19] for closely related results). We should moreover mention that the equation has no solution in positive integers x, y when $c = -1$, as can be inferred from the work of Nagell [26] and Cao [16].

The case when $c = q^{2n}$, where q is an odd prime, was studied in the recent paper [3] of Abu Muriefah. Let us first note that, for fixed n and $p \geq 5$, the Diophantine equation $px^2 + q^{2n} = y^p$

* Corresponding author.

E-mail addresses: alaradji@kfupm.edu.sa (A. Laradji), mignotte@math.u-strasbg.fr (M. Mignotte), tzanakis@math.uoc.gr (N. Tzanakis).

URL: <http://www.math.uoc.gr/~tzanakis> (N. Tzanakis).

and, more generally, the Diophantine equation $pX^2 + Y^{2n} = Z^p$, have at most finitely many solutions (x, q, y) and (X, Y, Z) , respectively. Indeed, in this case, $\frac{1}{2} + \frac{1}{2n} + \frac{1}{p} < 1$ and the claim follows from Theorem 2 of [20]. A main result in the aforementioned paper [3], namely, Theorem 3.1, states that the equation $5x^2 + q^{2n} = y^5$, has two families of solutions given by $y = \phi_{3k}, \phi_{3k+1}$ (or ψ_{3k+1}, ψ_{3k+2}), $k > 1$, where ϕ_k (respectively ψ_k) is the k th term of the Fibonacci sequence (respectively the Lucas sequence). However, straightforward computations show that the only Fibonacci or Lucas number $y < 1000$ satisfying the title equation when $p = 5$ is $y = 21$ with $x = 410$, $q = 1801$, $n = 1$, and, further, in $5 \times 183630^2 + 160201^2 = 181^5$, 160201 is prime and 181 is neither a Fibonacci nor a Lucas number. The same Theorem 3.1 of [3] states that, if $p > 3$ is a prime $\not\equiv 7 \pmod{8}$ and q is another odd prime, then there are no integer solutions (x, y, n) to the equation $px^2 + q^{2n} = y^p$ with $(x, y) = 1$. The proof of Theorem 3.1 in [3], just before its end, contains an obvious, non-rectifiable error, at case 2, when $-16apb^2$ is set equal to $-16apq^{2m}$ although $b = \pm q^j$ with $0 \leq j < m$. That the said proof is erroneous is also pointed out by P.G. Walsh in his review [30] of [3]. One of our aims in the present paper is to prove Abu Muriefah's assertion when $p \equiv 3 \pmod{8}$; see Theorem 2.3. Our proof, rather than rectifying Abu Muriefah's argument (this is probably impossible), goes through totally different lines. Unfortunately, our arguments cannot be extended to the case $p \equiv 1 \pmod{4}$.

As we revisited the title equation, we further discovered some new results, like Theorems 1.1, 3.2 and 4.1 which, we believe, merit one's attention. Moreover, since the powerful techniques of Sections 4 and 3 are also applicable (after the appropriate modifications) to Diophantine equations other than the ones treated in this paper, we thought it useful to expose them in some detail, enough for the reader to profit from them.

As we stated above, one of the main results of this paper is the following

Theorem 1.1. *Let q be an odd prime. If either $q \not\equiv 1 \pmod{600}$ or $q \leq 3 \cdot 10^9$, then there is no integer solution (x, y, n) to the equation*

$$5x^2 + q^{2n} = y^5, \quad x, y, n > 0. \quad (1)$$

Otherwise, there exists at most one integer solution (x, y, n) and if it actually exists, then it must satisfy the following conditions:

- (i) $n < 820$ and $\gcd(n, 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) = 1$.
- (ii) *There exists an integer v such that $x = 10v(80v^4 - 40v^2 + 1)$, $y = 20v^2 + 1$, $q^n = 2000v^4 - 200v^2 + 1$.*

Remark. If the prime q is of the form $q = 2000v^4 - 200v^2 + 1$ (the first few primes of this shape are 1801, 160201, 1245001, 4792201, 8179201), then $(x, y, n) = (10v(80v^4 - 40v^2 + 1), 20v^2 + 1, 1)$ is a solution to (1) and, according to the theorem, this is the only one (with $x, y > 0$). We have not been able, however, to find a prime q such that the corresponding equation (1) has a solution with $n > 1$. Therefore, we state the following

Conjecture. *If the prime q is not of the form $q = 2000v^4 - 200v^2 + 1$, then Eq. (1) has no solutions.*

The proof of Theorem 1.1 follows from a straightforward combination of Corollary 2.2 and Theorem 4.1, a second main result of our paper. In turn, the proof of Theorem 4.1 relies on a third main result, namely, Theorem 3.2 concerning the equation $5x^2 - 4 = y^n$ which is interesting for its own sake. Indeed, in recent years, important papers are devoted to equations of the form $x^2 + C = y^n$. One main strategy for attacking such equations is based on the so called *modular method* which has been successfully applied in quite a number of cases; see Chapter 15 (by S. Siksek) in H. Cohen's book [18], the survey article [4] and [14] and the references therein. For our equation $5x^2 - 4 = y^n$, the existence of the trivial solution $(x, y) = (1, 1)$ makes the modular approach unsuccessful and prevents us from giving the complete solution (x, y, n) . Thus, our Theorem 3.2 offers only a partial result which, at present, seems to be best possible.

2. The Diophantine equation $px^2 + q^{2n} = y^p$

The main results of this section are Proposition 2.1 and Theorem 2.3.

Proposition 2.1. *Let $p > 3$ be a prime number $\not\equiv 7 \pmod{8}$ and let q be an odd prime number. If x, y, n are positive integers with x, y relatively prime such that*

$$px^2 + q^{2n} = y^p, \quad (x, y) = 1, \quad n > 0, \quad (2)$$

then there exists a rational integer a such that

$$\pm q^n = \sum_{i=0}^{(p-1)/2} \binom{p}{2i+1} a^{p-2i-1} (-p)^{(p-2i-1)/2} \quad (3)$$

and

$$x = \sum_{i=0}^{(p-1)/2} \binom{p}{2i} a^{p-2i} (-p)^{(p-2i-1)/2}. \quad (4)$$

Proof. The condition $(x, y) = 1$ implies $p \neq q$ and the condition $p \not\equiv 7 \pmod{8}$ implies that y is odd.

We work in the imaginary quadratic field $K = \mathbb{Q}(\omega)$, where $\omega = \sqrt{-p}$. Eq. (2) factorizes as $(\omega x + q^n)(-\omega x + q^n) = y^p$ and, trivially, the factors in the left-hand side are relatively prime. This implies an ideal equation $\langle \omega x + q^n \rangle = \mathbf{I}^p$, where $\mathbf{I}$ is an integral ideal of K . Since the ideal-class number of K is strictly less than p (see p. 199 of [21]), the above ideal equation implies that $\mathbf{I}$ is a principal ideal, therefore we obtain the equation

$$x\omega + q^n = \alpha^p, \quad \alpha = a\theta + b, \quad \theta = \begin{cases} \omega & \text{if } p \equiv 1, 5 \pmod{8}, \\ \frac{1+\omega}{2} & \text{if } p \equiv 3 \pmod{8} \end{cases} \quad (5)$$

for some rational integers a and b . In case $p \equiv 3 \pmod{8}$ we write the above equation as $q^n - x + 2x\theta = (b + a\theta)^p$, implying $(b + a\theta)^p \equiv 0$ or $1 \pmod{2}$. From this, we see that a cannot be odd. For, otherwise, we would have θ^p or $(1 + \theta)^p \equiv 0$ or $1 \pmod{2}$. But we easily check that, for $k \not\equiv 0 \pmod{3}$, it is true that $\theta^k, (1 + \theta)^k \equiv \theta$ or $1 + \theta \pmod{2}$, a contradiction. Therefore, a in (5) is even and (5) is equivalent to the simpler equation

$$x\omega + q^n = \alpha^p, \quad \alpha = a\omega + b, \quad (6)$$

for some rational integers a and b of opposite parity since $y = a^2p + b^2$ is odd. Also, it is easy to see that $(pa, b) = 1$. If we put

$$\beta = -\bar{\alpha},$$

then

$$x = \frac{\alpha^p + \beta^p}{2\omega}, \quad \frac{q^n}{b} = \frac{\alpha^p - \beta^p}{\alpha - \beta}$$

and the fact that $(\alpha^p - \beta^p)/(\alpha - \beta)$ is an algebraic integer implies that b divides q^n (in $\mathbb{Z}$), hence $b = \pm q^j$ for some $j \in \{0, 1, \dots, n\}$.

At this point we note that the pair $(\alpha, -\beta)$ is a Lehmer pair for which

$$(\alpha^2 - \beta^2)^2 = -16pa^2b^2.$$

Concerning j appearing in the relation $b = \pm q^j$ (see a few lines above), we distinguish two cases.

(i) $j > 0$. Then, in the terminology of [9], $(\alpha, -\beta)$ is a p -defective pair. By Theorems 1.4 and C of [9] it easily follows that $p = 5$ is the only possibility. Then, by Theorem 1.3 of [9], either $20a^2 = \phi_{k-2\epsilon}$ for some $k \geq 3$, or $20a^2 = \psi_{k-2\epsilon}$ for some $k \neq 1$, where $\epsilon \in \{-1, 1\}$, $(\phi_n)_{n \geq 0}$ denotes the Fibonacci sequence and $(\psi_n)_{n \geq 0}$ is defined by $\psi_0 = 2$, $\psi_1 = 1$ and $\psi_n = \psi_{n-1} + \psi_{n-2}$ for $n \geq 2$. It is easily checked that, for every $n \geq 0$, $\psi_n \not\equiv 0 \pmod{5}$; therefore the second alternative must be excluded. On the other hand, by Théorème 1.3 of [12], a relation of the form $\phi_k = 5z^m$ with $m > 1$ and $z > 1$ is impossible, which excludes the first alternative as well.

(ii) $j = 0$, so that $b = \pm 1$. Then, equating rational and irrational parts in (6), we respectively obtain the relations (3) and (4). $\square$

Corollary 2.2. *If the integers x, y, q, n , where $(x, y) = 1$, q is an odd prime and $n \geq 1$, satisfy the equation*

$$5x^2 + q^{2n} = y^5 \tag{7}$$

then $(n, 6) = 1$, $q \equiv 1 \pmod{600}$ and there exists an integer v such that

$$x = 10v(80v^4 - 40v^2 + 1), \quad y = 20v^2 + 1, \quad q^n = 2000v^4 - 200v^2 + 1. \tag{8}$$

Proof. Applying Proposition 2.1 with $p = 5$ we obtain $\pm q^n = 125a^4 - 50a^2 + 1$ and $x = 5a(5a^4 - 10a^2 + 1)$. Obviously, the minus sign in the first equation is rejected and a is even. Putting $a = 2v$ in these relations we obtain the first and third relation in (8), and then the second relation results immediately.

We claim that n is odd. Indeed, otherwise $(a, q^{n/2})$ would be an integral point on the elliptic curve defined by $Y^2 = 125X^4 - 50X^2 + 1$. But this elliptic curve has zero rank and its only rational point is $(X, Y) = (0, \pm 1)$, which forces $q = 1$, a contradiction.

We also claim that n is prime to 3. Indeed, let us write the third equation (8) as $q^n + 4 = 5w^2$, where $w = 20v^2 - 1$. If n were divisible by 3, then the last equation could be written as $(5^2w)^2 = (5q^{n/3})^3 + 500$, again forcing $q = 1$, because it is well known since long (see, for example, Table 8 in [25]) that the only integral solutions (X, Y) to $Y^2 = X^3 + 500$ are $(X, Y) = (5, \pm 25)$.

Finally, we show that $q \equiv 1 \pmod{600}$. First, we write the third equation (8) as $q^n = 200v^2 \times (v^2 - 1) + 1$, which shows that $q^n \equiv 1 \pmod{600}$. Let r be the order of q modulo 600. Then r divides n , and since $\varphi(600) = 160$ and n is odd, we obtain $r = 1$ or $r = 5$. The latter case cannot hold, for, otherwise, $5x^2 = y^5 - (q^{2n/5})^5$, which has no proper solutions by Théorème 2(2) of [22]. We therefore conclude that $r = 1$ and $q \equiv 1 \pmod{600}$, as claimed. $\square$

Theorem 2.3. *Let p, q be odd primes with $p \equiv 3 \pmod{8}$ and $p > 3$. Then, the Diophantine equation*

$$px^2 + q^{2n} = y^p \tag{9}$$

has no positive integer solutions (x, y, n) with $(x, y) = 1$.

Proof. By the relation (3) we see that Eq. (9) implies

$$\pm q^n = \frac{(a\omega + 1)^p - (a\omega - 1)^p}{2}.$$

Let us consider the polynomial

$$f(x) := \frac{(\omega x + 1)^p - (\omega x - 1)^p}{2}.$$

Clearly, this is a polynomial in $\mathbb{Z}[x]$ of degree $p - 1$, with leading coefficient $-p^{(p+1)/2}$ and constant term 1.

First Claim: The polynomial $f(x)$ factorizes over $\mathbb{Q}[x]$ into two relatively prime polynomials $f_1(x), f_2(x) \in \mathbb{Z}[x]$, each of degree $(p - 1)/2$.

Proof: Let ζ be a primitive p th root of unity, i.e. a root of the p th cyclotomic polynomial $\Phi(x) = x^{p-1} + \dots + x + 1 = (x^p - 1)/(x - 1)$. Let also g be a primitive root mod p . Observe that the field $L = \mathbb{Q}(\zeta)$ contains ω . Indeed, it is a well-known fact that the Gauss sum $G = \sum_{t=1}^{p-1} (\frac{t}{p}) \zeta^t$ satisfies $G^2 = (-1)^{(p-1)/2} p$. Therefore, we can assume $\omega = G$. Below we will use the well-known fact that, in the field L we have the factorization into prime ideals $(p) = (\lambda)^{p-1}$, where $\lambda = 1 - \zeta$. For $\beta \in L$ we will write $w(\beta)$ to denote $v_\lambda(\beta)$, the exponent of λ in the prime factorization of β ; and for $b \in \mathbb{Q}$ we will write $v(b)$ to denote $v_p(b)$, the exponent of p in the prime factorization of b .

We have

$$f(x) = \prod_{k=1}^{p-1} \{(\omega x + 1) - \zeta^k(\omega x - 1)\},$$

from which it follows that the roots of $f(x)$ are exactly the following:

$$\frac{\omega}{p} \cdot \frac{1 + \zeta^k}{1 - \zeta^k}, \quad k = 1, \dots, p - 1.$$

Therefore,

$$f(x) = -p^{(p+1)/2} \prod_{k=1}^{p-1} \left(x - \frac{\omega}{p} \cdot \frac{1 + \zeta^k}{1 - \zeta^k} \right).$$

Let us put now

$$f_1(x) = p^{(p+1)/4} \prod_{j=0}^{(p-3)/2} \left(x - \frac{\omega}{p} \cdot \frac{1 + \zeta^{g^{2j}}}{1 - \zeta^{g^{2j}}} \right),$$

$$f_2(x) = -p^{(p+1)/4} \prod_{j=0}^{(p-3)/2} \left(x - \frac{\omega}{p} \cdot \frac{1 + \zeta^{g^{2j+1}}}{1 - \zeta^{g^{2j+1}}} \right),$$

so that $f(x) = f_1(x)f_2(x)$. We now show that the polynomials $f_i(x)$ have rational coefficients.

The Galois group of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ is cyclic generated by the automorphism σ , defined by $\sigma(\zeta) = \zeta^g$. Since $\omega \in \mathbb{Q}(\zeta) \setminus \mathbb{Q}$, we must have $\sigma(\omega) \neq \omega$, therefore, $\sigma(\omega) = -\omega$. Consequently, for the typical root of $f_1(x)$ we have

$$\sigma \left(\frac{\omega}{p} \cdot \frac{1 + \zeta^{g^{2j}}}{1 - \zeta^{g^{2j}}} \right) = -\frac{\omega}{p} \cdot \frac{1 + \zeta^{g^{2j+1}}}{1 - \zeta^{g^{2j+1}}} = \frac{\omega}{p} \cdot \frac{1 + \zeta^{g^{2j'}}}{1 - \zeta^{g^{2j'}}}, \quad (10)$$

where

$$j' \equiv \frac{p+1}{4} + j \pmod{\frac{p-1}{2}}$$

and we choose

$$j' = \begin{cases} \frac{p+1}{4} + j & \text{if } 0 \leq j < \frac{p-3}{4}, \\ \frac{p+1}{4} + j - \frac{p-1}{2} & \text{if } \frac{p-3}{4} \leq j \leq \frac{p-3}{2}, \end{cases}$$

so that j' runs (exactly once) through all values $0, 1, \dots, \frac{p-3}{2}$ as j runs through these values. Consequently, the coefficients of the polynomial $f_1(x)$ are fixed by σ , which implies that they belong to $\mathbb{Q}$; and similarly for $f_2(x)$. Actually, the coefficients of $f_1(x), f_2(x)$ are integers and we prove this as follows.

First, we show that the absolute value of the constant coefficient of both $f_1(x)$ and $f_2(x)$ is 1. Indeed, let b_i be the constant coefficient of $f_i(x)$. We already know that $b_i \in \mathbb{Q}$. Moreover, multiplying the right equalities (10) for $j = 0, \dots, (p-3)/2$ and then the resulting products in the two sides by $-p^{(p+1)/4}$, we obtain $b_2 = b_1$. But, $b_1 b_2$ is equal to the constant term of $f(x)$, which is 1. Therefore $1 = b_1 b_2 = b_1^2$, from which $b_1 = b_2 = \pm 1$.

Let us put now

$$g(x) = x^{p-1} f\left(\frac{1}{x}\right), \quad g_1(x) = x^{(p-1)/2} f_1\left(\frac{1}{x}\right), \quad g_2(x) = x^{(p-1)/2} f_2\left(\frac{1}{x}\right),$$

i.e. these are the reciprocal polynomials of $f(x), f_1(x)$ and $f_2(x)$, respectively. Since $f(x) = f_1(x) f_2(x)$, we also have $g(x) = g_1(x) g_2(x)$. Since the constant term of $f(x)$ is 1, $g(x)$ has leading coefficient 1; and since $f(x)$ has integer coefficients, so does $g(x)$. Therefore, the roots of $g(x)$ are algebraic integers. Analogously, the polynomials $g_i(x)$ have leading coefficients equal to ± 1 , their coefficients are rational numbers and their roots, being roots of $g(x)$, are algebraic integers. Therefore, these polynomials have coefficients in $\mathbb{Z}$; consequently, the same is true for the polynomials $f_i(x)$, as claimed.

Now, observe that $f_1(x)$ and $f_2(x)$ have no common roots, therefore they are relatively prime.

Second Claim: Let $\text{Res}(f_1, f_2)$ be the resultant of the polynomials f_1, f_2 . Then

$$\text{Res}(f_1, f_2) = \pm 2^{(p-1)^2/4} p^{(p^2-1)/8}. \quad (11)$$

Proof: We use the symbol Disc to denote the discriminant. We have

$$\text{Disc}(f) = \text{Disc}(f_1 f_2) = \text{Disc}(f_1) \text{Disc}(f_2) \text{Res}(f_1, f_2)^2.$$

By the right-most equality in (10) and the comments following it we see that $f_2(x) = 0$ iff $f_1(-x) = 0$, hence

$$\text{Disc}(f) = \text{Disc}(f_1 f_2) = \text{Disc}(f_1)^2 \text{Res}(f_1, f_2)^2. \quad (12)$$

Calculation of $\text{Disc}(f)$:

$$\text{Disc}(f) = p^{(2p-4)(p+1)/2} \prod_{1 \leq i < j \leq p-1} \left(\frac{\omega}{p} \cdot \frac{1+\zeta^i}{1-\zeta^i} - \frac{\omega}{p} \cdot \frac{1+\zeta^j}{1-\zeta^j} \right)^2$$

$$\begin{aligned}
&= p^{(p+1)(p-2)} \left(\frac{-1}{p} \right)^{(p-2)(p-1)/2} \prod_{1 \leq i < j \leq p-1} \left(\frac{2(\zeta^i - \zeta^j)}{(1 - \zeta^i)(1 - \zeta^j)} \right)^2 \\
&= -2^{(p-1)(p-2)} p^{(p-2)(p+3)/2} \prod_{1 \leq i < j \leq p-1} \left(\frac{\zeta^i - \zeta^j}{(1 - \zeta^i)(1 - \zeta^j)} \right)^2.
\end{aligned}$$

The right-most product in the last equality is a unit times $\lambda^{-(p-1)(p-2)}$, therefore, $w(\text{Disc}(f)) = (p-1)(p-2)(p+3)/2 - (p-1)(p-2) = (p-2)(p^2-1)/2$. But, since $\text{Disc}(f)$ is a rational integer, it follows that

$$\text{Disc}(f) = \pm 2^{(p-1)(p-2)} p^{(p-2)(p+1)/2}. \quad (13)$$

Calculation of $\text{Disc}(f_1)$:

$$\begin{aligned}
\text{Disc}(f_1) &= p^{(p-3)(p+1)/4} \prod_{0 \leq i < j \leq (p-3)/2} \left(\frac{\omega}{p} \cdot \frac{1 + \zeta^{g^{2i}}}{1 - \zeta^{g^{2i}}} - \frac{\omega}{p} \cdot \frac{1 + \zeta^{g^{2j}}}{1 - \zeta^{g^{2j}}} \right)^2 \\
&= p^{(p+1)(p-3)/4} \left(\frac{-1}{p} \right)^{(p-3)(p-1)/8} \prod_{0 \leq i < j \leq (p-3)/2} \left(\frac{2(\zeta^{g^{2i}} - \zeta^{g^{2j}})}{(1 - \zeta^{g^{2i}})(1 - \zeta^{g^{2j}})} \right)^2 \\
&= -2^{(p-1)(p-3)/4} p^{(p-3)(p+3)/8} \prod_{0 \leq i < j \leq (p-3)/2} \left(\frac{\zeta^{g^{2i}} - \zeta^{g^{2j}}}{(1 - \zeta^{g^{2i}})(1 - \zeta^{g^{2j}})} \right)^2.
\end{aligned}$$

The right-most product in the last equality is a unit times $\lambda^{-(p-1)(p-3)/4}$, therefore, $w(\text{Disc}(f_1)) = (p-1)(p-3)(p+3)/8 - (p-1)(p-3)/4 = (p-1)(p-3)(p+1)/8$. Since $\text{Disc}(f_1)$ is a rational integer, it follows that

$$\text{Disc}(f_1) = \pm 2^{(p-1)(p-3)/4} p^{(p-3)(p+1)/8}. \quad (14)$$

Now the relations (12), (13) and (14) imply the validity of the relation (11).

Third Claim: Among the integers $f_1(a)$, $f_2(a)$ one is equal to ± 1 and the other is equal to $\pm q^n$.

Proof: By Bezout's identity, there exist polynomials $h_1(x), h_2(x) \in \mathbb{Z}[x]$ (both of degree $< (p-1)/2$) such that

$$h_1(x)f_1(x) + h_2(x)f_2(x) = \text{Disc}(f_1, f_2) = \pm 2^{(p-1)^2/4} p^{(p^2-1)/8}.$$

We make the substitution $x \leftarrow a$ in this equality. By $f_1(a)f_2(a) = f(a) = \pm q^n$ and the fact that $(q, 2p) = 1$ (cf. beginning of the proof of Proposition 2.1), it follows that exactly one $f_i(a)$ is equal to ± 1 and the other is equal to $\pm q^n$.

Fourth Claim: If $f_i(a) = \pm 1$ for some $i \in \{1, 2\}$, then $a = 0$.

Proof: Let us put $f_1(x) = c_0 + c_1x + \dots + c_rx^r$, where $r = (p-1)/2$. We already know that $c_0 = \pm 1$ and $c_i \in \mathbb{Z}$ for all i . By the very definition of the polynomial f_1 , its roots are

$$\xi_j = \frac{1 + \zeta^j}{\omega(1 - \zeta^j)}, \quad j \in S,$$

where S is a complete set of quadratic residues mod p .

Since $\Phi(-1) = 1$ the numerator $1 + \zeta^j$ is a unit and it follows easily that

$$w(\xi_j) = -(p+1)/2.$$

Thus, for $k > 0$,

$$w(c_k) \geq -\frac{p+1}{2} \frac{p-1-2k}{2} + \frac{(p-1)(p+1)}{4} = \frac{k(p+1)}{2}.$$

Then, for $k \geq 1$, we have $v(c_k) = w(c_k)/(p-1) > 0$ and therefore

$$p|c_k, \quad k = 1, \dots, (p-1)/2. \quad (15)$$

Moreover, for $k \geq 2$, we have $v(c_k) \geq (p+1)/(p-1) > 1$, hence $v(c_k) \geq 2$ and we can write therefore

$$f_1(x) \equiv c_0 + c_1x \pmod{p^2x^2}. \quad (16)$$

Next, we prove that

$$v(c_1) = 1. \quad (17)$$

First, note that $f_2(x) = f_1(-x)$, which results from the fact that the polynomial f_1 is of odd degree, and the polynomials f_1 and f_2 have opposite leading coefficients and roots (cf. just before the relation (12)). These observations imply that $f_2(x) = c_0 - c_1x + c_2x^2 - c_3x^3 + \dots$.

Another observation is that $c_1 \neq 0$. Indeed, since $f(x) = f_1(x)f_2(x)$, the coefficient of x^2 in $f(x)$ is $2c_0c_2 + c_1^2$. On the other hand, by the initial definition of $f(x)$, the coefficient of x^2 is $-p\binom{p}{2}$, which is odd, because $p \equiv 3 \pmod{4}$. Therefore, c_1 is odd; in particular, it is non-zero.

A third fact—which is a bit more than an observation—is that

$$|c_1| < p^2. \quad (18)$$

If we prove this, then, in combination with the relation (15) and the fact that $c_1 \neq 0$, we will conclude that $v(c_1) = 1$.

Proof of (18): Let $g_1(x)$ be, as before, the reciprocal of the polynomial $f_1(x)$. Then c_1 is equal, up to sign, with the sum of the roots of $g_1(x)$. But the roots of $g_1(x)$ are the reciprocals of the roots of $f_1(x)$, i.e. they are equal to ξ_j^{-1} , $i = 1, \dots, (p-1)/2$. Therefore (remember that S is a complete set of residues mod p),

$$|c_1| \leq \sqrt{p} \sum_{j \in S} \left| \frac{1 - \zeta^j}{1 + \zeta^j} \right| = \sqrt{p} \sum_{j \in S} \left| \tan \frac{\pi j}{p} \right| = \sqrt{p} \sum_{j \in S} \frac{1}{\left| \tan \frac{\pi(p-2j)}{2p} \right|}.$$

Since $\left| \frac{\pi(p-2j)}{2p} \right| < \frac{\pi}{2}$, it follows that $\left| \tan \frac{\pi(p-2j)}{2p} \right| > \frac{\pi}{2p} |p-2j|$, hence,

$$|c_1| < \frac{2p\sqrt{p}}{\pi} \sum_{j \in S} \frac{1}{|p-2j|}.$$

Note that, as j runs through the set S , the numbers $|p-2j|$ are distinct mod p , for, if $|p-2j_1| \equiv |p-2j_2| \pmod{p}$ with $j_1, j_2 \in S$ and $j_1 \neq j_2$, then, necessarily, $j_2 = -j_1$, which implies that -1

is a quadratic residue mod p , a contradiction. Therefore, the set $\{|p - 2j|: j \in S\}$ is a subset of $\{1, \dots, p - 1\}$ with cardinality $(p - 1)/2$. It is clear, therefore, that

$$\sum_{j \in S} \frac{1}{|p - 2j|} \leq \sum_{k=1}^{(p-1)/2} \frac{1}{k} < \frac{3}{2} + \log \frac{p-1}{4},$$

from which we obtain

$$|c_1| < \frac{2p\sqrt{p}}{\pi} \left(\frac{3}{2} + \log \frac{p-1}{4} \right).$$

This upper bound for $|c_1|$ clearly implies $|c_1| < p^2$, as claimed.

Final step of the proof of Theorem 2.3: By our third claim above, $f_1(a)$ or $f_2(a)$ must be ± 1 . Since $f_2(a) = -f_1(-a)$, we may suppose that $f_1(a) = \pm 1$, i.e. $c_0 + c_1a + c_2a^2 + \dots = \pm 1$. Remember that $c_0 = \pm 1$, therefore, $c_0 + c_1a + c_2a^2 + \dots = \pm c_0$. The $-$ sign implies $\pm 2 + c_1a + c_2a^2 + \dots = 0$, clearly impossible, in view of (15). The $+$ sign implies $0 = c_1a + c_2a^2 + \dots$. If $a \neq 0$, then, taking also into account (16), we obtain $0 = c_1 \pmod{p^2}$ which contradicts (17). This forces $a = 0$ and then, by (3), $q^n = \pm 2$, a contradiction. $\square$

3. The equation $5x^2 - 4 = y^n$

The third relation (8), written as $q^n = 5(20v^2 - 1)^2 - 4$, naturally leads to the study of the more general equation

$$5x^2 - 4 = y^n, \quad |x|, y > 1, n > 2, \quad (19)$$

in the integer unknowns x, y, n , where x and y have not, of course, the same meaning as the x, y in Eq. (7).

First, let n be even. It is well known that the positive integer solutions of $5X^2 - 4 = Y^2$ are given by $X = F_{2k+1}$, $Y = L_{2k+1}$ for $k > 0$, where F denotes the Fibonacci and L the Lucas sequence; notice that $k = 0$ gives $y = 1$ which is excluded. Since it is known that the only Lucas number which is a pure power is $L_3 = 4$ [13, Theorem 2], it follows that the only solution (x, y, n) of Eq. (19) with even n is $(2, 2, 4)$.

From now on we suppose that n is odd.

If $n = 3$, then $(25x)^2 - 500 = (5y)^3$. It is well known that the only integral solutions (X, Y) to $Y^2 = X^3 + 500$ are $(X, Y) = (5, \pm 25)$, corresponding to $y = 1$, which has been excluded by hypothesis. Hence we may assume that $\gcd(n, 3) = 1$, in particular $n \geq 5$.

If x is even then $5x^2 - 4 \equiv -4, 16, 12 \pmod{32}$ implying $n \leq 4$, which has already been excluded. Hence x and y are odd.

Now we work in the field $K = \mathbb{Q}(\theta)$, where $\theta = \sqrt{5}$. From now on and until the end of the paper we view K as embedded into the real numbers with $\theta \mapsto \sqrt{5} = 2.2360679\dots$. The ring of integers in K is $\mathbf{I} = \{(x + y\theta)/2; x, y \in \mathbb{Z} \text{ with } x \equiv y \pmod{2}\}$, $\varepsilon = (1 + \sqrt{5})/2$ is the fundamental unit. In K unique factorization holds. Throughout this section, for $\alpha \in K$, α' will always denote the algebraic conjugate of α . We factorize Eq. (19) over the field K

$$5x^2 - 4 = (x\theta - 2)(x\theta + 2). \quad (20)$$

If p is a (rational) prime divisor of y , then $5x^2 - 4 = y^n$ implies that p is odd and, clearly, 5 is a quadratic residue mod p . It follows that p splits in K and $p \equiv \pm 1 \pmod{5}$. Therefore y factorizes in $\mathbf{I}$ as $y = \pi\pi'$, where we can choose $\pi > 0$ (then π' is also positive). Notice also that $y^n \equiv 1 \pmod{5}$, hence $y \equiv 1 \pmod{10}$ (remember that y and n are odd) and $y \geq 11$.

Without loss of generality, we assume that x is positive. Since x is odd, $x\theta + 2$ and $x\theta - 2$ are coprime with $x\theta > y^{n/2} \geq 11^{5/2}$. Hence, there exists $k \in \mathbb{Z}$ such that $x\theta + 2 = \varepsilon^k \pi^n$. Writing $k = \ell n + k_1$ with $-(n-1)/2 \leq k_1 \leq (n-1)/2$, we have $x\theta + 2 = \varepsilon^{k_1} (\varepsilon^\ell \pi)^n = \varepsilon^{k_1} \pi_1^n$, where $\pi_1 = \varepsilon^\ell \pi$. The conjugate relation is $-x\theta + 2 = \varepsilon'^{k_1} \pi_1'^n$ and summing the two relations we get

$$\varepsilon^{k_1} \pi_1^n + \varepsilon'^{k_1} \pi_1'^n = 4. \quad (21)$$

We have $\pi_1 = u + v\theta$ or $\pi_1 = (u + v\theta)/2$, where $u, v \in \mathbb{Z}$ are unknown and in the second case uv is odd. Then, for fixed n and k_1 we obtain from (21)

$$T_{k_1}(u, v) := \varepsilon^{k_1} (u + v\theta)^n + \varepsilon'^{k_1} (u - v\theta)^n = 4 \text{ or } 2^{n+2}, \quad (22)$$

where, in the second case, uv is odd. Note that the left-hand side of (22) is a homogeneous polynomial in $\mathbb{Z}[u, v]$ of degree n , hence the relation (22) implies a Thue equation. Since $T_{-k_1}(u, v) = (-1)^{k_1} T_{k_1}(u, -v)$, it suffices to consider the Thue equations $T_{k_1}(u, v) = \pm 4$ and $T_{k_1}(u, v) = \pm 2^{n+2}$ with $k_1 = 0, 1, \dots, (n-1)/2$, where, in the second equation, uv is odd. Moreover, since the degree of the form T_{k_1} is odd, we can ignore the minus sign in the right-hand sides. Using the above Thue equations we will prove that there are no solutions (x, y, n) to (19) with $n \in \{5, 7, 11, 13\}$. Actually, we will show that for these values of n the Thue equations $T_{k_1}(u, v) = 2^{n+2}$ with uv odd, and $T_{k_1}(u, v) = 4$ are impossible for all $k_1 = 0, 1, \dots, (n-1)/2$. For every n as above, the method is practically the same. However, as one can guess, the case $n = 13$ is somewhat more complicated; so we briefly expose this case in order to illustrate how we work. Numerous Thue equations of degree n arise. A practical method for the solution of such equations has been developed since long by Tzanakis and de Weger [28] which later was improved by Bilu and Hanrot [8] and implemented in PARI (<http://pari.math.u-bordeaux.fr/>) and MAGMA [10,15]. We use either of these packages to solve the Thue equations that arise.

We assume now that $n = 13$ and we consider all k_1 's in $\{0, 1, \dots, 6\}$.

$k_1 = 0$: Since $T_0(u, v)$ is reducible, our equations are treated by elementary means; no solutions arise.

$k_1 = 1$: Both equations $T_1(u, v) = 4, 2^{15}$ are easily solved.

$k_1 = 2$: The congruences $T_2(u, v) \equiv 4, 2^{15} \pmod{13^2}$ are impossible.

$k_1 = 3$: The equation $T_3(u, v) = 2^{15}$ with uv odd implies solvability of the congruence $T_3(x, 1) \equiv 0 \pmod{2^{14}}$. But, as it is easily checked, this congruence has no solutions. The equation $T_3(u, v) = 4$ remains. Since $T_3(u, v) = 4u^{13} + \dots$, we multiply by 2^{11} and we obtain a Thue equation $u'^{13} + 65u'^{12}v + \dots + 320000000v^{13} = 2^{13}$, whose only solution is $(u', v) = (2, 0)$ which we obviously reject.

$k_1 = 4$: Now, $T_4(u, v) = 7u^{13} + \dots + 234375v^{13}$. On multiplying by 7^{12} we obtain monic Thue equations with right-hand sides $4 \cdot 7^{12}$ and $2^{15} 7^{12}$. No solutions are returned.

$k_1 = 5$: Similarly to the case $k_1 = 2$, both congruences $T_5(u, v) \equiv 4, 2^{15} \pmod{13^2}$ are impossible.

$k_1 = 6$: All coefficients of $T_6(u, v)$ are even and $\frac{1}{2}T_6(u, v) = 9u^{13} + 260u^{12}v + \dots + 312500v^{13} = T'_6(u, v)$, say. We thus have the Thue equations $T'_6(u, v) = 2^{14}$ with uv odd, and $T'_6(u, v) = 2^2$. The first equation implies solvability of the congruence $T'_6(x, 1) \equiv 0 \pmod{2^{13}}$ with x odd, which is impossible. For the second equation we are obliged to multiply by 3^{24} in order to obtain a monic Thue equation, as required by both PARI and MAGMA. The resulting equation is treated with some "effort" by MAGMA and no solutions are returned. On the other hand, PARI after several hours was still "struggling", so we gave up.

The computational difficulties arising above, when $k_1 = 6$ show the limitation of the method and, indeed, for $n = 17$ the computational difficulties for the solution of the resulting Thue equations, at present, seem to be insurmountable.

Summing up our results so far, we have the following theorem.

Proposition 3.1. *There are no solutions (x, y, n) to Eq. (19) with n divisible by at least one of the primes 3, 5, 7, 11 or 13. The only solution (x, y, n) to Eq. (19) with even n is $(\pm 2, 2, 4)$.*

Computing a first upper bound for n . We now fix a solution (x, y, n) of Eq. (19), where, in view of Proposition 3.1, we can assume that $n \geq 17$. Obviously, we can also assume that n is prime. Based on the few observations just after Eq. (20), but relaxing the condition $x > 0$, we see that there exists a set $\mathcal{P}$ consisting of (unordered) sets $\{\pi, \pi'\}$ such that $\pi > 0$, $\pi\pi' = y$ and, if $\{\pi_1, \pi'_1\}$ and $\{\pi_2, \pi'_2\}$ are distinct elements of $\mathcal{P}$, then π_2, π'_2 are non-associated to both π_1, π'_1 .

We modify $\mathcal{P}$ as follows: Let $\{\pi, \pi'\} \in \mathcal{P}$. There exists precisely an $m \in \mathbb{Z}$ such that $\varepsilon^m \leq \sqrt{\varepsilon y}/\pi < \varepsilon^{m+1}$. The last relation is equivalent to $\varepsilon^{2m-1}\pi^2 \leq y < \varepsilon^{2m+1}\pi^2$. On putting $\varepsilon^m\pi = \pi_1$ we obtain

$$\frac{\pi_1}{\sqrt{\varepsilon}} \leq \sqrt{y} < \pi_1\sqrt{\varepsilon}, \quad \text{or, equivalently,} \quad \sqrt{\frac{y}{\varepsilon}} < \pi_1 \leq \sqrt{\varepsilon y}. \quad (23)$$

Note that $\pi'_1 = (-1)^m \varepsilon^{-m} \pi'$, so that $\pi_1|\pi'_1| = y$. On multiplying the first relation (23) by $|\pi'_1|$ we get $\frac{y}{\sqrt{\varepsilon}} \leq |\pi'_1|\sqrt{y} < y\sqrt{\varepsilon}$, hence $\sqrt{\frac{y}{\varepsilon}} \leq |\pi'_1| < \sqrt{y\varepsilon}$. The last relation combined with the second relation (23) implies $\max\{|\pi_1|/|\pi'_1|, |\pi'_1|/|\pi_1|\} \leq \varepsilon$ and, certainly, the left-hand side of the last inequality is > 1 . We make the substitution $\pi \leftarrow \pi_1$ or $\pi \leftarrow |\pi'_1|$ according as $\pi_1/|\pi'_1|$ is > 1 or < 1 , respectively. In this way, an “adjusted” set $\mathcal{P}_1$ replaces the set $\mathcal{P}$ containing elements $\{\pi, \pi'\}$ such that,

$$\pi > 0, \quad \pi|\pi'| = y, \quad 1 < \pi/|\pi'| \leq \varepsilon. \quad (24)$$

Now, in view of the relation (20) and the fact that the two factors in the left-hand side are relatively prime, we must have an ideal equation $\langle 2 + x\theta \rangle = \langle \pi \rangle^n$ or $\langle 2 + x\theta \rangle = \langle \pi' \rangle^n$ for some $\{\pi, \pi'\} \in \mathcal{P}_1$, and then $\langle -2 + x\theta \rangle = \langle \pi' \rangle^n$ or $\langle -2 + x\theta \rangle = \langle \pi \rangle^n$, respectively. By choosing the appropriate sign for x we may assume that $\langle 2 + x\theta \rangle = \langle \pi \rangle^n$, from which it follows that

$$2 + x\theta = \sigma \varepsilon^k \pi^n \quad \text{for some } k \in \mathbb{Z} \text{ and } \sigma \in \{-1, 1\}, \quad (25)$$

and

$$x\theta - 2 = \frac{y^n}{x\theta + 2} = \frac{\pi^n |\pi'|^n}{\sigma \varepsilon^k \pi^n} = \sigma \varepsilon^{-k} |\pi'|^n. \quad (26)$$

By (25) and (26) we obtain

$$\varepsilon^{2k} \left(\frac{\pi}{|\pi'|} \right)^n - 1 = \frac{\sigma \varepsilon^k \pi^n}{\sigma \varepsilon^{-k} |\pi'|^n} - 1 = \frac{x\theta + 2}{x\theta - 2} - 1 = \frac{4}{x\theta - 2}. \quad (27)$$

We have $5x^2 = y^n + 4$, from which $|x\theta| > y^{n/2}$.

Now we put

$$\Lambda = 2k \log \varepsilon - n \log \frac{|\pi'|}{\pi}, \quad (28)$$

so that $\Lambda = \log(\varepsilon^{2k} (\frac{\pi}{|\pi'|})^n)$ and now, by (27),

$$|e^\Lambda - 1| = \frac{4}{|x\theta - 2|} \leq \frac{4}{|x|\theta - 2} < \frac{4}{y^{n/2} - 2} < \frac{4.0001}{y^{n/2}}.$$

Notice that the right-most side is less than $5.63 \cdot 10^{-9}$ in view of the fact that $y \geq 11$ and $n \geq 17$. Therefore,

$$|\Lambda| < 1.01 |e^\Lambda - 1| < \frac{4.0402}{y^{n/2}}.$$

On the other hand, since the ideals $\langle \pi \rangle$ and $\langle \pi' \rangle$ are distinct, $\pi/|\pi'|$ is not a unit and, consequently, $\Lambda \neq 0$. Thus,

$$0 < |\Lambda| < \frac{4.0402}{y^{n/2}} \quad (29)$$

and

$$\log |\Lambda| < -\frac{n}{2} \log y + 1.3963. \quad (30)$$

Now we compare k and n that appear in the linear form Λ . Since $\log \varepsilon$ and $\log \frac{\pi}{\pi'}$ are both positive and, by (29), $|\Lambda|$ is very small, it follows that k is negative. By (29), $|\Lambda| < 7.6 \times 10^{-6}$, therefore, in view also of (24),

$$|k| = -k = -\frac{\Lambda}{2 \log \varepsilon} + \frac{n}{2 \log \varepsilon} \log \frac{\pi}{|\pi'|} < 7.9 \times 10^{-6} + \frac{n}{2 \log \varepsilon} \log \varepsilon = 7.9 \times 10^{-6} + \frac{n}{2},$$

hence

$$|k| \leq \frac{n}{2}. \quad (31)$$

Next, we consider the algebraic number $\eta := \frac{\pi}{|\pi'|}$ appearing in Λ . This number is a root of the polynomial

$$(\pi X - |\pi'|)(|\pi'|X - \pi) = yX^2 - (\pi^2 + \pi'^2)X + y = yX^2 - (a^2 \pm 2y)X + y \in \mathbb{Z},$$

where $a = \pi + \pi' \in \mathbb{Z}$. From this we easily see that

$$h(\eta) < \frac{1}{2}(\log y + \log \varepsilon). \quad (32)$$

Finally, we are ready to calculate a first upper bound for n using Corollary 2 of [23]. In view of the relations (32) and (24) it is easy to estimate the quantities that are involved in that corollary. Choosing the parameter m that appears in the corollary equal to 20, and taking into account that $\max(2|k|, |n|) = n$ (cf. 31), we easily find that, if $n \geq 15100$, then

$$\log |\Lambda| \geq 78.8 \left(\log n + \log \frac{\log y + \log \varepsilon + 1}{\log y + \log \varepsilon} + 0.38 \right)^2 (\log y + \log \varepsilon).$$

This, combined with (30), gives

$$78.8 \left(\log n + \log \frac{\log y + \log \varepsilon + 1}{\log y + \log \varepsilon} + 0.38 \right)^2 (\log y + \log \varepsilon) - \frac{n}{2} \log y + 1.3963 > 0. \quad (33)$$

Since $y \geq 11$, we easily check that the inequality (33) can hold only if

$$n < 2.2 \times 10^4. \quad (34)$$

Proving that solutions with “small” y cannot exist. Now we go back to our Eq. (19) and we assume that (x, y) is a positive solution. It is easily checked that this positiveness restriction does not prevent us from obtaining again the relations (27) and (29). We write the last inequality in the following shape:

$$\left| \frac{\log \eta}{\log \varepsilon} - \frac{2k}{n} \right| < \frac{4.0402}{n \log \varepsilon \cdot y^{n/2}}, \quad \eta := \frac{\pi}{\pi'}.$$

The right-hand side is, obviously, less than $1/(2n^2)$, which shows that $2k/n$ is a convergent to the continued fraction expansion of $\log \eta / \log \varepsilon$ and, moreover, the denominator of this convergent is less than 10^5 , in view of (34). Let $a_0, a_1, a_2, \dots$ be the partial quotients and $p_0/q_0, p_1/q_1, p_2/q_2, \dots$ the convergents to that expansion. Let h be the first subscript such that $q_h \geq 10^5$. Then, $2k/n = p_m/q_m$ for some $m \in \{0, \dots, h-1\}$. We have now

$$\frac{1}{(a_{i+1} + 2)q_i^2} < \left| \frac{\log \eta}{\log \varepsilon} - \frac{p_i}{q_i} \right|,$$

hence,

$$\frac{1}{(a_{i+1} + 2)n^2} < \left| \frac{\log \eta}{\log \varepsilon} - \frac{2k}{n} \right| < \frac{4.0402}{n \log \varepsilon \cdot y^{n/2}},$$

from which it follows that

$$4.0402(A + 2)n > \log \varepsilon \cdot y^{n/2}, \quad A := \max\{a_0, a_1, \dots, a_h\}. \quad (35)$$

For every $y \equiv 1 \pmod{10}$ with $y < 3 \cdot 10^9$ and for every π as above (there are 2^m such η 's, where m is the number of rational prime divisors of y), we compute η and the continued fraction expansion of the real number $\log \eta / \log \varepsilon$, and we check the validity of the relation (35). These computations can be performed with the routines of either PARI or MAGMA. We stress the fact that an ordinary precision is sufficient since the denominators of the checked convergents have at most 10 decimal digits. The whole task took around 30 hours of computations with PARI in a usual PC; with MAGMA it would take more time. It turns out that, except possibly if $n \leq 11$, this relation is *not* satisfied. But we already know that $n \geq 17$, hence we conclude:

No solutions to (x, y, n) to (19) exist with $n \geq 17$ and $y \leq 3 \cdot 10^9$.

Obtaining a smaller upper bound for n . Now, we know that $y > 3 \cdot 10^9$ (this is very important!) and we apply Theorem 2 of [23] to our linear form Λ . In the notation of that theorem, we choose $\rho = 15.7$ and $\mu = 0.57$. We obtain a new lower bound for $|\Lambda|$ which, as before, we combine with (30) to obtain a complicated relation in which the only parameters that are present are y and n . Since $y > 3 \cdot 10^9$, we check that n must necessarily be at most 6404. Falling from the upper bound (34) to $n \leq 6404$ is already a considerable improvement, but we can do much better. We turn to the main theorem of [23], namely Theorem 1. Its application is somewhat complicated, as one has to choose appropriately various parameters $\rho, \mu, R_1, R_2, S_1, S_2, K, L$, but it's worth the trouble! The strategy is the following: Once we have the lower bound $y > 3 \cdot 10^9$ and an upper bound for n , we choose our parameters above in order to obtain a smaller upper bound for n . We repeat the process with this reduced upper bound and new parameters, and so on, as in Table 1. In Table 1 we omit the values of K and L because we always choose

$$L = R_1 S_1, \quad K = \max \left\{ \left\lceil \frac{R_2 S_2 - 1}{R_1 S_1} \right\rceil, 2 \right\}.$$

Table 1
The choice of parameters in Theorem 1 of [23].

ρ	μ	R_1	S_1	R_2	S_2	starting ub for n	reduced ub for n
11	0.6	1	20	400	110	6404	5802
11	0.6	1	20	300	100	5802	3956
11	0.6	1	20	211	80	3956	2226
10	0.57	1	15	205	79	2226	1949
9.95	0.57	1	15	198	75	1949	1783
10	0.555	2	8	195	75	1783	1713
10	0.56	2	8	186	66	1713	1452
10	0.555	2	7	184	63	1452	1358
10	0.555	3	5	178	60	1358	1251
10	0.555	4	4	173	60	1251	1216
11.01	0.6	4	4	172	49	1216	1113
10.09	0.59	4	3	170	48	1113	1054
11	0.6	6	2	165	46	1054	1003
10.9	0.6	7	2	162	46	1003	980
15.7	0.57	4	3	149	42	980	901
15.555	0.565	4	3	149	42	901	890
15.3	0.565	4	3	149	42	890	885
16.05	0.58	4	3	145	41	885	878
16.05	0.58	4	3	145	41	885	878
16.045	0.579	4	3	145	41	878	877
16.045	0.579	6	2	142	41	877	859
16.05	0.578	6	2	142	41	859	858
16.051	0.577	6	2	142	41	858	856
16.052	0.576	6	2	142	41	856	855
16.053	0.575	6	2	142	41	855	853
16.054	0.5744	6	2	142	41	853	852
16.054	0.5743	6	2	145	40	852	849
16.042	0.5788	6	2	144	40	849	848
16.042	0.5788	6	2	160	35	848	825
16.03	0.575	6	2	160	35	825	820

The choice of the remaining parameters requires experiments; we cannot expose a systematic strategy for choosing them.

No further reduction of the upper bound of n was possible.

Summing up all the results of Section 3 we obtain the following theorem.

Theorem 3.2. Any integer solution (x, y, n) of the equation $5x^2 - 4 = y^n$ with $y > 1$ and $n > 2$ must satisfy the following:

- (i) $n < 820$.
- (ii) The prime divisors of n are ≥ 17 and ≤ 811 .
- (iii) $y > 3 \cdot 10^9$.

Remark. In recent years, the so-called “modular approach” to certain types of Diophantine equations—the Fermat equation being one of them—turned out to be very succesful; see, for example, S. Siksek’s “The modular approach to Diophantine equations”, Chapter 15 in [18]. Our equation $5x^2 - 4 = y^n$ resembles the Lebesgue–Nagell equation $x^2 + D = y^n$, to which the modular method applies succesfully in most cases; see [14]. However, as mentioned in [14], the method is not succesful when $D = -a^2 \pm 1$ because, in that case, there exists an obvious solution valid for every n . In the case of our equation we face a similar situation: the existence of the solution $(x, y) = (1, 1)$ for every n makes the application of the modular method “hopeless”, according to S. Siksek (private communication).

4. The equation $5x^2 - 4 = y^n$ when y is prime

The main result of this section is the following:

Theorem 4.1. Let q be an odd prime. Then, for the solutions (x, n) of the equation

$$5x^2 - 4 = q^n, \quad x > 0, n > 0, n \neq 2 \quad (36)$$

the following are true:

- (i) If $q \not\equiv 1 \pmod{10}$, no solutions exist.
- (ii) If $q \leq 3 \cdot 10^9$, no solutions with $n > 2$ exist.
- (iii) If $(q+4)/5 = \square$, then $(x, n) = (\sqrt{\frac{q+4}{5}}, 1)$ is the only solution.
- (iv) If $(q+4)/5 \neq \square$, then at most one solution exists.
- (v) No solutions exist with $n > 820$.
- (vi) No solutions exist with n divisible by a prime from the set $\{2, 3, 5, 7, 11, 13\}$.

The proof of this theorem follows from a straightforward combination of Theorem 3.2, already proved in Section 3 and Proposition 4.2, below. Therefore, the present section is essentially devoted to the proof of this proposition.

As noted in the beginning of Section 3, the third relation (8), written as $5(20v^2 - 1)^2 - 4 = q^n$, led us to the more general equation (19) for which Theorem 3.2 holds. In this theorem, y is general and not necessarily prime as the equation $5(20v^2 - 1)^2 - 4 = q^n$ would suggest. In this section, however, we will add the extra restriction that the unknown y in Eq. (19) be a prime, say $y = q$, and we will prove the following theorem.

Proposition 4.2. If q is an odd prime, then the equation

$$5x^2 = q^n + 4, \quad x, n \text{ positive integers, } n \text{ odd} \quad (37)$$

has at most one solution if $(q+4)/5$ is not a perfect square and exactly one solution, namely, $(x, n) = (\sqrt{(q+4)/5}, 1)$ if $(q+4)/5$ is a perfect square.

Remark. It is easy to see that the relation (37) implies $q \equiv 1 \pmod{10}$.

Proof. The proof of Proposition 4.2 will be completed in three steps.

Step 1: The gap between two solutions of (37). This step consists in proving that, if two solutions (x, n) , and (x', n') exist, with $n' > n$, then n' must be “very large” compared to n ; see (42). We need first the following result.

Lemma 4.3. Let x be a positive integer and assume that

$$2 + x\sqrt{5} = \xi^a, \quad (38)$$

where ξ is an algebraic integer in $\mathbb{Q}(\sqrt{5})$ and a is an integer > 1 . Then, $\xi = \frac{1+\sqrt{5}}{2}$, $a = 3$, $x = 1$.

Proof. There are two possibilities for ξ : (I) Either $\xi = \frac{b+c\sqrt{5}}{2}$ with b, c odd integers, or (II) $\xi = b + c\sqrt{5}$ with b, c arbitrary integers.

After expansion of the right-hand side of (38) we obtain

$$b^a + 5c^2 \binom{a}{2} b^{a-2} + \dots = \begin{cases} 2^{a+1} & \text{in case (I),} \\ 2 & \text{in case (II).} \end{cases}$$

It follows from this that, if a is even, then an odd power of 2 is a square mod 5 which is impossible. Therefore, a is odd and

$$b^a + 5c^2 \binom{a}{2} b^{a-2} + \dots + 5^{\frac{a-1}{2}} c^{a-1} \binom{a}{a-1} b = \begin{cases} 2^{a+1} & \text{in case (I),} \\ 2 & \text{in case (II).} \end{cases}$$

Case (II) is impossible. Indeed, note that in the left-hand side all exponents of b are odd and all exponents of c are even, hence $b > 0$. Also, b divides 2, hence $b = 1$ or 2. If $b = 1$ then an obviously impossible congruence mod 5 results; and if $b = 2$ then $2^a \leq 2$ which implies $a = 1$, contrary to the hypothesis.

In case (I) we have, as before, $b > 0$, b is odd and $b|2^{a+1}$. Hence, $b = 1$ and we have

$$2^{a+1} = 1 + 5 \binom{a}{2} c^2 + \dots + 5^{\frac{a-1}{2}} \binom{a}{a-1} c^{a-1} \geq 2^{a+1}$$

where the last inequality is strict for every c , if $a \geq 5$ and for every c with $|c| > 1$ when $a = 3$. Thus, to avoid the contradiction we must conclude that $a = 3$ and $|c| = 1$ from which it easily follows that $c = 1$ and $\xi = (1 + \sqrt{5})/2$. This completes the proof of Lemma 4.3. $\square$

We put $\theta = (1 + \sqrt{5})/2$, $\theta' = (1 - \sqrt{5})/2$. These are the roots of the polynomial $x^2 - x - 1$ and θ is the fundamental unit of the ring of integers of $\mathbb{Q}(\theta)$. In general, for any $\alpha \in \mathbb{Q}(\theta)$ we denote by α' the conjugate of α under the isomorphism $\theta \mapsto \theta'$.

Assume now that (x, n) is a solution to Eq. (37). Then $(2 + x\sqrt{5})(2 - x\sqrt{5}) = -q^n$ and it is clear that the factors in the left-hand side are relatively prime as algebraic integers of $\mathbb{Q}(\theta)$. Also, every (rational) prime dividing q factors into two distinct prime ideals. It follows then that there exists an algebraic integer σ with norm $\pm q$ such that the following ideal relation is true: $(2 + x\sqrt{5}) = (\sigma)^n$. Then, for some $r \in \mathbb{Z}$ we have the element equation $2 + x\sqrt{5} = \pm \theta^r \sigma^n$ and since we can assume without loss of generality that $\sigma > 0$, we finally get

$$2 + x\sqrt{5} = \theta^r \sigma^n \quad \text{along with the conjugate relation } 2 - x\sqrt{5} = \theta'^r \sigma'^n.$$

Combining the last two relations we obtain

$$0 < \delta := \left(\frac{\theta'}{\theta}\right)^r \left(\frac{\sigma'}{\sigma}\right)^n + 1 = \frac{4}{\theta^r \sigma^n} = \frac{4}{2 + x\sqrt{5}} < \frac{1}{2}.$$

Then, $\frac{1}{2} < 1 - \delta = -\left(\frac{\theta'}{\theta}\right)^r \left(\frac{\sigma'}{\sigma}\right)^n < 1$ and in view of the inequality $|\log(1 - x)| < |x|(1 + |x|)$ (valid for $|x| < 1/2$) we obtain

$$\left| -r \log \left| \frac{\theta}{\theta'} \right| + n \log \left| \frac{\sigma'}{\sigma} \right| \right| < \delta(1 + \delta), \quad \delta = \frac{4}{2 + x\sqrt{5}} = \frac{4}{2 + \sqrt{q^n + 4}} < \frac{4}{q^{n/2}}. \quad (39)$$

Now, let (x', n') another solution to (37) with $n' > n$, n' odd and $x' > 0$ (hence, $x' > x$). Exactly as before we have a relation $2 + x'\sqrt{5} = \theta^{r'} \sigma'^{n'}$ for a convenient $r' \in \mathbb{Z}$ and

$$\left| -r' \log \left| \frac{\theta}{\theta'} \right| + n' \log \left| \frac{\sigma'}{\sigma} \right| \right| < \delta'(1 + \delta'), \quad \delta' = \frac{4}{2 + \sqrt{q^{n'} + 4}} < \frac{4}{q^{n'/2}} < \delta. \quad (40)$$

Putting $u = \log |\theta/\theta'| = \log((3 + \sqrt{5})/2)$ and eliminating the term $\log |\sigma'/\sigma|$ from the inequalities (39) and (40) we get $|-rn' + r'n|u < n'\delta(1 + \delta) + n\delta'(1 + \delta') < 2n'\delta(1 + \delta)$, i.e.

$$|-rn' + r'n| < \frac{2n'}{u} \delta(1 + \delta). \quad (41)$$

The left-hand side in (41) is non-zero. Indeed, in the opposite case we would have $\frac{r}{n} = \frac{r'}{n'} =$ (say) $\frac{r_1}{n_1}$ with $(r_1, n_1) = 1$. Then, $r = ar_1, n = an_1, r' = br_1, n' = bn_1$ for some positive odd integers a, b with $a < b$ and, moreover, $2 + x'\sqrt{5} = (\theta^{r_1}\sigma^{n_1})^b$. By Lemma 4.3 we conclude that $x' = 1$, contrary to the fact that $x' > x > 1$.

We conclude therefore that the left-hand side of (41) is ≥ 1 , from which it follows that

$$n' > \frac{u}{2}\delta^{-1}(1+\delta)^{-1}, \quad (42)$$

which shows that, the larger solution n' is “far away” from the smaller solution n ; specifically, it is of the size of $q^{n/2}$. This fact will play an important role below.

Step 2: Application of hypergeometric polynomials. At this second step we adapt to our equation the method of F. Beukers in [6] and [7]. As a result we prove Lemma 4.4 below, after which the final step for the proof of Proposition 4.2 is not difficult. In that method one uses as a tool the hypergeometric polynomials, the properties of which we remind immediately below.

Given the real numbers α, β, γ where γ is not zero or a negative integer, we define the *hypergeometric function* (with parameters α, β, γ)

$$F(\alpha, \beta, \gamma, z) = 1 + \frac{\alpha\beta}{\gamma}z + \sum_{k=2}^{\infty} \frac{1}{k!} \frac{\alpha(\alpha+1)\cdots(\alpha+k-1)\beta(\beta+1)\cdots(\beta+k-1)}{\gamma(\gamma+1)\cdots(\gamma+k-1)} z^k$$

which converges for every complex number z with $|z| < 1$ and, in case that $\gamma > \alpha + \beta$, it also converges for $z = 1$. Let $n_2 > n_1 > 0$ be integers. Put $n = n_1 + n_2$ and define

$$G(z) = F(-n_2 - 1/2, -n_1, -n, z), \quad H(z) = F(-n_1 + 1/2, -n_2, -n, z).$$

By the definition of G it is easy to see that

$$G(z) = \sum_{k=0}^{n_1} \binom{n_2 + 1/2}{k} \binom{n_1}{k} \binom{n}{k}^{-1} (-z)^k,$$

which, in particular, shows that, for any real number $z < 0$, $G(z)$ is positive. We will use the following properties:

- (1) $G(z)$ and $H(z)$ are polynomials in z of degrees n_1 and n_2 , respectively. Moreover, the polynomials $\binom{n}{n_1}G(4z)$ and $\binom{n}{n_1}H(4z)$ have integer coefficients.
- (2) $|G(z) - (1-z)^{1/2}H(z)| < G(1)|z|^{n+1}$ for $|z| < 1$.
- (3) $G(1) < G(z) < G(0) < 1$ for $0 < z < 1$.
- (4) If $G^*(z)$ is the polynomial resulting from $G(z)$ when n_1, n_2 are respectively replaced by $n_1 + 1, n_2 + 1$ and $H^*(z)$ is defined analogously, then

$$G^*(z)H(z) - G(z)H^*(z) = cz^{n+1}$$

for some non-zero constant c .

- (5) $|G(z)| < (1 + \frac{|z|}{2})^{n_2+1}$ for any z .

For the proof of the first four properties see Lemmas 1, 2, 3 and 4 in [6]. For the proof of the fifth property see relation (1.10), p. 226 of [29]. Now we are in a position to prove the main result of this step.

Lemma 4.4. Let (x, n) be a solution to (37), where, as always, $x > 0$ and $n \geq 1$ is odd; we assume, moreover, that $q^n > 600$. Let r, s be positive integers such that $q^n \geq 2^{6+4s/r}$ and define the positive real number v by means of the relation

$$q^{nv} = 2.007 \times (4.03q^n)^{r/s}.$$

Finally, let $N = q^{n'}$ where $n' > n$ and let y be any integer. Then,

$$\left| \frac{y\sqrt{5}}{N^{1/2}} - 1 \right| > \frac{0.27}{q^{n(3+v/2)}} q^{n/s} N^{-(1+v)/2}.$$

Proof. Let $n_2 > n_1$ be positive integers which will be specified later and $m = n_1 + n_2$. Put $z = -q^{-n}$. Then, $|4z| < 1$ so that $G(4z)$ and $H(4z)$ are meaningful. By properties (2) and (3) of the polynomials G and H we have

$$\left| G(4z) - H(4z) \left(1 + \frac{4}{q^n} \right)^{1/2} \right| < G(1) \left(\frac{4}{q^n} \right)^{m+1} < \left(\frac{4}{q^n} \right)^{m+1},$$

hence

$$\left| \binom{m}{n_1} G(4z) - \binom{m}{n_1} H(4z) \frac{x\sqrt{5}}{q^{n/2}} \right| < \binom{m}{n_1} \left(\frac{4}{q^n} \right)^{m+1}. \quad (43)$$

By property (1) and the fact that $G(x) > 0$ for any negative real number x ,

$$\binom{m}{n_1} G(4z) = \frac{A}{q^{nm_1}} \quad \text{for some positive } A \in \mathbb{Z}$$

and similarly,

$$\binom{m}{n_1} H(4z) = \frac{B}{q^{nm_2}} \quad \text{for some } B \in \mathbb{Z}.$$

Then, (43) implies $\left| \frac{A}{q^{nm_1}} - \frac{Bx}{q^{nm_2}} \frac{\sqrt{5}}{q^{n/2}} \right| < \binom{m}{n_1} \left(\frac{4}{q^n} \right)^{m+1}$, from which

$$\left| 1 - \frac{Bx\sqrt{5}}{Aq^{n(n_2-n_1+1/2)}} \right| < 2^{m-1} \frac{q^{nm_1}}{A} \frac{2^{2(m+1)}}{q^{n(m+1)}} = \frac{2^{3m+1}}{Aq^{n(n_2+1)}}.$$

Now, let us put $\epsilon = \left| \frac{y\sqrt{5}}{N^{1/2}} - 1 \right|$, so that, from the above inequality we have

$$\left| \frac{y}{N^{1/2}} - \frac{Bx}{Aq^{n(n_2-n_1+1/2)}} \right| < \frac{1}{\sqrt{5}} \left(\epsilon + \frac{2^{3m+1}}{Aq^{n(n_2+1)}} \right). \quad (44)$$

Let $\lambda = \lceil \frac{n'-n}{2n} \rceil$. Then,

$$q^{n(\lambda-1)} < \left(\frac{N}{q^n} \right)^{1/2} \leq q^{n\lambda}. \quad (45)$$

Now comes the moment to choose n_1, n_2 . First we choose n_1 to satisfy

$$\frac{r}{s}\lambda \leq n_1 \leq \frac{r}{s}\lambda + \frac{2s-1}{s}. \quad (46)$$

We must keep in mind that there are exactly two consecutive positive integers in the interval $[r\lambda/s, (r\lambda + 2s - 1)/s]$; this is a simple exercise. Choose now n_2 by setting $n_2 = n_1 + \lambda > n_1$ and remember that $m = n_1 + n_2 = 2n_1 + \lambda$. Moreover, we will need below that the left-hand side of (44) be non-zero. In the next lines we show that we can choose n_1 in such a way that this requirement be satisfied.

Suppose that for the smaller integer n_1 in the interval $[r\lambda/s, (r\lambda + 2s - 1)/s]$ the left-hand side of (44) is zero. Then, we can repeat the above process with $n'_1 := n_1 + 1$ in place of n_1 (n'_1 still belongs to this interval), $n'_2 := n_2 + 1$ in place of n_2 and $m' := n'_1 + n'_2$ in place of m , so that the polynomials G and H will be replaced by G^* and H^* respectively, and the integers A, B by some other integers, say, A^*, B^* . Then, we will obtain an inequality analogous to (44), namely,

$$\left| \frac{y}{N^{1/2}} - \frac{B^*x}{A^*q^{n(n'_2-n'_1+1/2)}} \right| < \frac{1}{\sqrt{5}} \left(\epsilon + \frac{2^{3m'+1}}{A^*q^{n(n'_2+1)}} \right).$$

If the left-hand side were again zero, then we would have $B/A = B^*/A^*$ (note that $n'_2 - n'_1 = n_2 - n_1$), which would easily imply that $z = -4/q^n$ is a zero of the function $G^* \cdot H - G \cdot H^*$ and this contradicts property (4) of the polynomials G, H . We conclude therefore that for at least one integer n_1 satisfying (46), the left-hand side of (44) is non-zero and from now on we assume that we have selected such an n_1 .

We now rewrite the term $Aq^{n(n_2-n_1+1/2)}$ appearing in the left-hand side of (44). We first observe that (45) implies $q^{n'/2} \leq q^{n(\lambda+1/2)}$ which shows that $q^{n(2\lambda+1)} = q^n q^{2\mu}$ for some non-negative integer μ . Consequently, on putting $q^\mu = A_0$ (a positive integer), we have

$$Aq^{n(n_2-n_1+1/2)} = Aq^{n(\lambda+1/2)} = Aq^{n'/2} A_0 = A_0 A N^{1/2}.$$

Going back to (44), we get

$$\begin{aligned} \frac{1}{\sqrt{5}} \left(\epsilon + \frac{2^{3m+1}}{Aq^{n(n_2+1)}} \right) &> \left| \frac{y}{N^{1/2}} - \frac{Bx}{Aq^{n(n_2-n_1+1/2)}} \right| = \left| \frac{y}{N^{1/2}} - \frac{Bx}{A_0 A N^{1/2}} \right| = \frac{|A_0 A y - Bx|}{A_0 |A| N^{1/2}} \\ &\geq \frac{1}{A_0 |A| N^{1/2}} = \frac{1}{|A| q^{n(\lambda+1/2)}}, \end{aligned}$$

from which

$$\epsilon |A| q^{n(\lambda+1/2)} + 2^{3m+1} q^{-n(n_1+1/2)} > \sqrt{5}. \quad (47)$$

We estimate separately the second summand in the left-hand side of (47). By the hypothesis on the lower bound of q^n and (45) we have

$$\frac{2^{3m+1}}{q^{nn_1}} < \frac{2^{6n_1+3\lambda+1}}{q^{nn_1}} \leq \frac{2^{6n_1+3\lambda+1}}{2^{(6+4s/r)n_1}} = 2^{3\lambda+1-4sn_1/r} \leq 2^{3\lambda+1-4\lambda} = 2^{1-\lambda} \leq 1,$$

which shows that the second summand in the left-hand side of (47) is $\leq q^{-n/2} < 600^{-1/2}$. This shows that the first summand in the left-hand side of (47) is larger than $5^{1/2} - 600^{-1/2} > 2.195$. Then, remembering also how A has been defined and using property (5) of the polynomial G , we get

$$\begin{aligned}
2.195 &\leq \epsilon |A| q^{n(\lambda+1/2)} = \epsilon q^{n(n_1+\lambda+1/2)} \binom{m}{n_1} |G(-4/q^n)| \\
&< \epsilon q^{n(n_1+\lambda+1/2)} \cdot 2^{m-1} \left(1 + \frac{2}{q^n}\right)^{n_2+1} \\
&\leq \epsilon q^{n(n_1+\lambda+1/2)} \cdot 2^{m-1} \left(1 + \frac{2}{q^n}\right)^m = \epsilon q^{n/2} q^{n(n_1+\lambda)} \cdot \frac{1}{2} \left(2 + \frac{4}{q^n}\right)^m \\
&< \frac{\epsilon}{2} q^{n/2} q^{n(n_1+\lambda)} \times 2.007^m \quad (\text{since } q^n > 600) \\
&= \frac{\epsilon}{2} q^{n/2} q^{n\lambda(1+n_1/\lambda)} \times 2.007^{\lambda(1+2n_1/\lambda)} \\
&\leq \frac{\epsilon}{2} q^{n/2} q^{n\lambda(\frac{r}{s} + \frac{2s-1}{\lambda s} + 1)} \times 2.007^{\lambda(\frac{2r}{s} + \frac{4s-2}{\lambda s} + 1)} \\
&= \frac{\epsilon}{2} q^{n/2} q^{n(2s-1)/s} \times 2.007^{(4s-2)/s} \cdot (q^{n(1+r/s)} \times 2.007^{1+2r/s})^\lambda \\
&< \frac{\epsilon}{2} q^{n/2} q^{n(2s-1)/s} \times 2.007^{(4s-2)/s} \cdot (2.007 \cdot (4.03q^n)^{r/s} q^n)^\lambda \\
&= \frac{\epsilon}{2} q^{n/2} q^{n(2s-1)/s} \times 2.007^{(4s-2)/s} \cdot q^{n(1+\nu)\lambda} \quad (\text{by the definition of } \nu) \\
&< \frac{\epsilon}{2} q^{n/2} q^{n(2s-1)/s} \times 2.007^4 \cdot q^{n(1+\nu)\lambda},
\end{aligned}$$

from which we immediately get

$$0.27q^{n(-\frac{5}{2} + \frac{1}{s})} < \epsilon q^{n\lambda(1+\nu)} < \epsilon (Nq^n)^{(\nu+1)/2}$$

(the right-most inequality being true because $q^{n\lambda} < (Nq^n)^{1/2}$ in view of (45)), and hence the claimed lower bound for $\epsilon = \lfloor \frac{\nu\sqrt{5}}{N^{1/2}} - 1 \rfloor$. This completes the proof of Lemma 4.4. $\square$

Step 3: Completion of the proof of Theorem 4.2. Assume that, if $(q+4)/5$ is not a perfect square there exists a solution to Eq. (37) and if $(q+4)/5$ is a perfect square there exists a solution to this equation besides the obvious one which results from the relation $5(\sqrt{(q+4)/5})^2 = q+4$. Thus, in both cases, our assumptions in particular imply that there exists a solution (x_0, n_0) with $n_0 > 1$, hence, by Theorem 3.2, we must have $q > 3 \cdot 10^9$. Let (x, n) be the least solution to Eq. (37). In order to prove the theorem, we will assume that a larger solution (x', n') to (37) exists and we will arrive at a contradiction.

We put $N = q^{n'}$, so that $N + 4 = 5x'^2$, from which we get

$$\frac{4}{N} = \left(\frac{\sqrt{5}x'}{N^{1/2}} - 1\right) \left(\frac{\sqrt{5}x'}{N^{1/2}} + 1\right) = \left(\frac{\sqrt{5}x'}{N^{1/2}} - 1\right) \left(\frac{\sqrt{N+4}}{\sqrt{N}} + 1\right) > 2 \left(\frac{\sqrt{5}x'}{N^{1/2}} - 1\right),$$

therefore

$$0 < \frac{\sqrt{5}x'}{N^{1/2}} - 1 < \frac{2}{N}.$$

We apply Lemma 4.4 with $y = x'$, $r = 1$, $s = 2$; then it is easy to check that $\nu < 0.7178$ and by the conclusion of the lemma and the last displayed inequality we get

$$2N^{-1} > \frac{\sqrt{5}x'}{N^{1/2}} - 1 > 0.27 \times q^{-n(5+\nu)/2} N^{-(1+\nu)/2},$$

hence

$$\frac{(1-\nu)}{2}m' \log q < \log(7.408) + \frac{5+\nu}{2}n \log q < \frac{5.627+\nu}{2}n \log q,$$

from which

$$n' < \frac{5.627+\nu}{1-\nu}n.$$

On the other hand, recalling that $u = \log((3 + \sqrt{5})/2)$ and $\delta = \frac{4}{2+\sqrt{q^n+4}}$, we have in view of (42),

$$\begin{aligned} n' &> \frac{u}{2}\delta^{-1}(1+\delta)^{-1} = \frac{u}{2} \cdot \frac{2+\sqrt{q^n+4}}{4} \left(1 + \frac{4}{2+\sqrt{q^n+4}}\right)^{-1} \\ &= \frac{u}{8} \cdot \frac{(2+\sqrt{q^n+4})^2}{6+\sqrt{q^n+4}} > \frac{u}{8} \cdot \frac{(2+q^{n/2})^2}{6+q^{n/2}} > 0.12 \times \frac{(2+q^{n/2})^2}{6+q^{n/2}}. \end{aligned}$$

Combining this lower bound for n' with (47), we get the following relation:

$$0.12 \times \frac{(2+q^{n/2})^2}{6+q^{n/2}} < \frac{5.627+\nu}{1-\nu}n.$$

By the definition of ν , $(q^n)^\nu = 2.007 \times (4.03q^n)^{1/2}$. Solving for ν and substituting into the above inequality we obtain

$$n \frac{6.127n \log q + \gamma}{0.5n \log q - \gamma} > 0.12 \frac{(2+q^{n/2})^2}{6+q^{n/2}}, \quad \gamma = \log(2.007 \cdot 4.03^{0.5}). \quad (48)$$

However, in view of the large size of q we easily check that (48) is *not* satisfied and this contradiction proves that the solution (x', n') cannot exist. $\square$

References

- [1] F. Abu Muriefah, On the Diophantine equation $Ax^2 + 2^{2m} = y^n$, *Int. J. Math. Math. Sci.* 20 (1997) 299–304.
- [2] F. Abu Muriefah, On the Diophantine equation $px^2 + 3^n = y^p$, *Tamkang J. Math.* 31 (2000) 79–84.
- [3] F. Abu Muriefah, On the Diophantine equation $px^2 + q^{2m} = y^p$, *J. Number Theory* 128 (2008) 1670–1675.
- [4] F. Abu Muriefah, Y. Bugeaud, The Diophantine equation $x^2 + C = y^n$: A brief overview, *Rev. Colombiana Math.* 40 (2006) 31–37.
- [5] N. Adachi, The Diophantine equation $x^2 \pm ly^2 = z^l$ connected with Fermat's last theorem, *Tokyo J. Math.* 11 (1988) 85–94.
- [6] F. Beukers, On the generalized Ramanujan–Nagell equation I, *Acta Arith.* 38 (1981) 389–410.
- [7] F. Beukers, On the generalized Ramanujan–Nagell equation II, *Acta Arith.* 39 (1981) 113–123.
- [8] Y. Bilu, G. Hanrot, Solving Thue equations of high degree, *J. Number Theory* 60 (1996) 373–392.
- [9] Y. Bilu, G. Hanrot, 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.
- [10] W. Bosma, J. Cannon, C. Playoust, The Magma Algebra System I. The user language, *J. Symbolic Comput.* 24 (3–4) (1997) 235–265.
- [11] E. Brown, Diophantine equations of the form $ax^2 + Db^2 = y^p$, *J. Reine Angew. Math.* 291 (1977) 118–127.
- [12] Y. Bugeaud, M. Mignotte, S. Siksek, Sur les nombres de Fibonacci de la forme $q^k y^p$, *C. R. Acad. Sci. Paris Ser. I* 339 (2004) 327–330.
- [13] Y. Bugeaud, M. Mignotte, S. Siksek, Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers, *Ann. of Math.* 163 (2006) 969–1018.
- [14] Y. Bugeaud, M. Mignotte, S. Siksek, Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell equation, *Compos. Math.* 142 (2006) 31–62.
- [15] J. Cannon, W. Bosma (Eds.), *Handbook of Magma Functions*, Edition 2.13, University of Sydney, 2006, 4350 pp.
- [16] Z. Cao, On the Diophantine equation $x^p - y^p = Dz^2$, *Northeast Math. J.* 2 (1986) 219–227.
- [17] Z. Cao, On the Diophantine equation $x^p + 2^{2m} = py^2$, *Proc. Amer. Math. Soc.* 128 (2000) 1927–1931.

- [18] H. Cohen, Number Theory, vol. II: Analytic and Modern Tools, Grad. Texts in Math., vol. 240, Springer, New York, 2007.
- [19] J.H.E. Cohn, The Diophantine equation $x^p + 1 = py^2$, Proc. Amer. Math. Soc. 131 (2003) 13–15.
- [20] H. Darmon, A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, Bull. Lond. Math. Soc. 27 (1995) 513–543.
- [21] A. Faisant, L' équation du second degré, Hermann, Paris, 1991.
- [22] A. Kraus, Une question sur les équations $x^m - y^m = Rz^n$, Compos. Math. 132 (2002) 1–26.
- [23] M. Laurent, Linear forms in two logarithms and interpolation determinants II, Acta Arith. 133 (2008) 325–348.
- [24] M. Le, On the Diophantine equation $2^n + px^2 = y^p$, Proc. Amer. Math. Soc. 123 (1995) 321–326.
- [25] H. London, R. Phinkelstein, On Mordell's Equation $y^2 - k = x^3$, Bowling Green State University, Bowling Green, OH, 1973.
- [26] T. Nagell, Sur l'impossibilité de quelques équations a deux indéterminées, Norsk Mat. Forenings Skrifter (1) 13 (1921) 65–82.
- [27] S. Rabinowitz, The solutions of $3y^2 \pm 2^n = x^3$, Proc. Amer. Math. Soc. 69 (1978) 213–218.
- [28] N. Tzanakis, B.M.M. de Weger, On the practical solution of the Thue equation, J. Number Theory 31 (1989) 99–132.
- [29] N. Tzanakis, J. Wolfskill, On the Diophantine equation $y^2 = 4q^n + 4q + 1$, J. Number Theory 23 (1986) 219–237.
- [30] P.G. Walsh, Mathematical Reviews, MR2419187 (2009d:11057).