ON THE DIOPHANTINE EQUATION $x^2 + q^{2m} = 2y^p$

SZ. TENGELY

ABSTRACT. In this paper we consider the Diophantine equation $x^2 + q^{2m} = 2y^p$ where m, p, q, x, y are integer unknowns with $m > 0$, p and q are odd primes and $\gcd(x, y) = 1$. We prove that there are only finitely many solutions (m, p, q, x, y) for which y is not a sum of two consecutive squares. We study the above equation for fixed y and in particular solve the case $y = 17$ completely. We also study the equation for fixed q and resolve the equation for $q = 3$.

1. INTRODUCTION

There are many results in the literature concerning the Diophantine equation

$$Ax^2 + p_1^{z_1} \cdots p_s^{z_s} = By^n,$$

where A, B are given non-zero integers, $p_1, \ldots, p_s$ are given primes and $n, x, y, z_1, \ldots, z_s$ are integer unknowns with $n > 2$, x and y coprime and non-negative, and $z_1, \ldots, z_s$ non-negative, see e.g. [1], [20], [2], [21], [22], [4], [3], [8], [9], [12], [15], [16], [17], [19], [18], [25]. Here the elegant result of Bilu, Hanrot and Voutier [7] on the existence of primitive divisors of Lucas and Lehmer numbers has turned out to be a very powerful tool. Using this result Luca [16] solved completely the Diophantine equation $x^2 + 2^a 3^b = y^n$. Le [14] obtained necessary conditions for the solutions of the equation $x^2 + p^2 = y^n$ in positive integers x, y, n with $\gcd(x, y) = 1$ and $n > 2$. He also determined all solutions of this equation for $p < 100$. In [25] Pink considered the equation $x^2 + (p_1^{z_1} \cdots p_s^{z_s})^2 = 2y^n$, and gave an explicit upper bound for n depending only on $\max p_i$ and s. The equation $x^2 + 1 = 2y^n$ was solved by Cohn [11]. Pink and Tengely [26] considered the equation $x^2 + a^2 = 2y^n$. They gave an upper bound for the exponent n depending only on a, and completely resolved the equation with $1 \le a \le 1000$ and $3 \le n \le 80$. In the present paper we study the equation $x^2 + q^{2m} = 2y^p$ where m, p, q, x, y are integer unknowns with $m > 0$, p and q odd primes and x and y coprime. In Theorem 1 we show that all but finitely many solutions are of a special type. Theorem 2 provides bounds for p. Theorem 3 deals with the case of fixed y, we completely resolve the equation $x^2 + q^{2m} = 2 \cdot 17^p$. Theorem 6 deals with the case of fixed q. It is proved that if the Diophantine equation $x^2 + 3^{2m} = 2y^p$ with $m > 0$ and p prime admits a coprime integer solution (x, y), then $(x, y, m, p) \in \{(13, 5, 2, 3), (79, 5, 1, 5), (545, 53, 3, 3)\}$. It means that the equation $x^2 + 3^m = 2y^p$ in copime integers is completely solved because solutions clearly do not exist when m is odd.

2. A FINITENESS RESULT

Consider the Diophantine equation

$$x^2 + q^{2m} = 2y^p, \tag{1}$$

where $x, y \in \mathbb{N}$ with $\gcd(x, y) = 1, m \in \mathbb{N}$ and p, q are odd primes and $\mathbb{N}$ denotes the set of positive integers. Since the case $m = 0$ was solved by Cohn [11] (he proved that the equation has only the solution $x = y = 1$ in positive integers) we may assume without

2000 *Mathematics Subject Classification.* Primary 11D61; Secondary 11Y50.

Key words and phrases. Diophantine equations.

loss of generality that $m > 0$. If $q = 2$, then it follows from $m > 0$ that $\gcd(x, y) > 1$, therefore we may further assume that q is odd.

Theorem 1. *There are only finitely many solutions* (x, y, m, q, p) *of* (1) *with* $\gcd(x, y) = 1, x, y \in \mathbb{N}$, *such that* y *is not a sum of two consecutive squares,* $m \in \mathbb{N}$ *and* $p > 3, q$ *odd primes.*

Remark. The question of finiteness if y is a sum of two consecutive squares is interesting. The following examples show that very large solutions can exist.

y	p	q
5	5	79
5	7	307
5	13	42641
5	29	1811852719
5	97	2299357537036323025594528471766399
13	7	11003
13	13	13394159
13	101	224803637342655330236336909331037067112119583602184017999
25	11	69049993
25	47	378293055860522027254001604922967
41	31	4010333845016060415260441

In these examples $m = 1$.

All solutions of (1) with small q^m have been determined in [27].

Lemma 1. *Let* q *be an odd prime and* $m \in \mathbb{N} \cup \{0\}$ *such that* $3 \leq q^m \leq 501$. *If there exist* $(x, y) \in \mathbb{N}^2$ *with* $\gcd(x, y) = 1$ *and an odd prime* p *such that* (1) *holds, then*

$$\begin{aligned}(x, y, q, m, p) \in \big\{&(3, 5, 79, 1, 5), (9, 5, 13, 1, 3), (13, 5, 3, 2, 3), (55, 13, 37, 1, 3),\\ &(79, 5, 3, 1, 5), (99, 17, 5, 1, 3), (161, 25, 73, 1, 3), (249, 5, 307, 1, 7),\\ &(351, 41, 11, 2, 3), (545, 53, 3, 3, 3), (649, 61, 181, 1, 3), (1665, 113, 337, 1, 3),\\ &(2431, 145, 433, 1, 3), (5291, 241, 19, 1, 3), (275561, 3361, 71, 1, 3)\big\}.\end{aligned}$$

Proof. This result follows from Corollary 1 in [27]. □

We introduce some notation. Put

$$\delta_4 = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4, \\ -1 \text{ if } p \equiv 3 \pmod 4. \end{cases} \tag{2}$$

and

$$\delta_8 = \begin{cases} 1 \text{ if } p \equiv 1 \text{ or } 3 \pmod 8, \\ -1 \text{ if } p \equiv 5 \text{ or } 7 \pmod 8. \end{cases} \tag{3}$$

Since $\mathbb{Z}[i]$ is a unique factorization domain, (1) implies the existence of integers u, v with $y = u^2 + v^2$ such that

$$\begin{aligned} x &= \Re((1 + i)(u + iv)^p) =: F_p(u, v),\\ q^m &= \Im((1 + i)(u + iv)^p) =: G_p(u, v). \end{aligned} \tag{4}$$

Here F_p and G_p are homogeneous polynomials in $\mathbb{Z}[X, Y]$.

Lemma 2. *Let* F_p, G_p *be the polynomials defined by* (4). *We have*

$$\begin{aligned} (u - \delta_4 v) &\mid F_p(u, v),\\ (u + \delta_4 v) &\mid G_p(u, v). \end{aligned}$$

Proof. This is Lemma 3 in [27]. □

Lemma 2 and (4) imply that there exists a $k \in \{0, 1, \dots, m\}$ such that either

$$\begin{aligned} u + \delta_4 v &= q^k, \\ H_p(u, v) &= q^{m-k}, \end{aligned} \tag{5}$$

or

$$\begin{aligned} u + \delta_4 v &= -q^k, \\ H_p(u, v) &= -q^{m-k}, \end{aligned} \tag{6}$$

where $H_p(u, v) = \frac{G_p(u,v)}{u+\delta_4 v}$.

For all solutions with large q^m we derive an upper bound for p in case of $k = m$ in (5) or (6) and in case of $q = p$.

Theorem 2. *If* (1) *admits a relatively prime solution* $(x, y) \in \mathbb{N}^2$ *then we have*

$$\begin{aligned} &p \le 3803 \text{ if } u + \delta_4 v = \pm q^m, q^m \ge 503, \\ &p \le 3089 \text{ if } p = q, \\ &p \le 1309 \text{ if } u + \delta_4 v = \pm q^m, m \ge 40, \\ &p \le 1093 \text{ if } u + \delta_4 v = \pm q^m, m \ge 100, \\ &p \le 1009 \text{ if } u + \delta_4 v = \pm q^m, m \ge 250. \end{aligned}$$

We shall use the following lemmas in the proof of Theorem 2. The first result is due to Mignotte [7, Theorem A.1.3]. Let α be an algebraic number, whose minimal polynomial over $\mathbb{Z}$ is $A \prod_{i=1}^{d} (X - \alpha^{(i)})$. The absolute logarithmic height of α is defined by

$$h(\alpha) = \frac{1}{d} \left(\log |A| + \sum_{i=1}^{d} \log \max(1, |\alpha^{(i)}|) \right).$$

Lemma 3. *Let* α *be a complex algebraic number with* $|\alpha| = 1$, *but not a root of unity, and* $\log \alpha$ *the principal value of the logarithm. Put* $D = [\mathbb{Q}(\alpha) : \mathbb{Q}]/2$. *Consider the linear form*

$$\Lambda = b_1 i\pi - b_2 \log \alpha,$$

where b_1, b_2 *are positive integers. Let* λ *be a real number satisfying* $1.8 \le \lambda < 4$, *and put*

$$\begin{aligned} &\rho = e^{\lambda}, \quad K = 0.5\rho\pi + Dh(\alpha), \quad B = \max(13, b_1, b_2), \\ &t = \frac{1}{6\pi\rho} - \frac{1}{48\pi\rho(1 + 2\pi\rho/3\lambda)}, \quad T = \left(\frac{1/3 + \sqrt{1/9 + 2\lambda t}}{\lambda} \right)^2, \\ &H = \max\Big\{ 3\lambda, D \left(\log B + \log \left(\frac{1}{\pi\rho} + \frac{1}{2K} \right) - \log \sqrt{T} + 0.886 \right) + \\ &+ \frac{3\lambda}{2} + \frac{1}{T} \left(\frac{1}{6\rho\pi} + \frac{1}{3K} \right) + 0.023 \Big\}. \end{aligned}$$

Then

$$\log |\Lambda| > -(8\pi T \rho \lambda^{-1} H^2 + 0.23)K - 2H - 2\log H + 0.5\lambda + 2\log\lambda - (D+2)\log 2.$$

The next result can be found as Corollary 3.12 at p. 41 of [23].

Lemma 4. *If* $\Theta \in 2\pi\mathbb{Q}$, *then the only rational values of the tangent and the cotangent functions at* Θ *are* $0, \pm 1$.

Proof of Theorem 2. Without loss of generality we assume that $p > 1000$ and $q^m \geq 503$. We give the proof of Theorem 2 in the case $u + \delta_4 v = \pm q^m, q^m \geq 503$, the proofs of the remaining four cases being analogous. From $u + \delta_4 v = \pm q^m$ we get

$$\frac{503}{2} \leq \frac{q^m}{2} \leq \frac{|u| + |v|}{2} \leq \sqrt{\frac{u^2+v^2}{2}} = \sqrt{\frac{y}{2}},$$

which yields that $y \geq \frac{q^{2m}}{2} > 126504$. Hence

$$\left|\frac{x + q^m i}{x - q^m i} - 1\right| = \frac{2 \cdot q^m}{\sqrt{x^2 + q^{2m}}} \leq \frac{2\sqrt{y}}{y^{p/2}} = \frac{2}{y^{\frac{p-1}{2}}}. \tag{7}$$

We have

$$\frac{x + q^m i}{x - q^m i} = \frac{(1+i)(u+iv)^p}{(1-i)(u-iv)^p} = i\left(\frac{u+iv}{u-iv}\right)^p. \tag{8}$$

If $\left|i\left(\frac{u+iv}{u-iv}\right)^p - 1\right| > \frac{1}{3}$ then $6 > y^{\frac{p-1}{2}}$, which yields a contradiction with $p > 1000$ and $y > 126504$. Thus $\left|i\left(\frac{u+iv}{u-iv}\right)^p - 1\right| \leq \frac{1}{3}$. Since $|\log z| \leq 2|z-1|$ for $|z - 1| \leq \frac{1}{3}$, we obtain

$$\left|i\left(\frac{u+iv}{u-iv}\right)^p - 1\right| \geq \frac{1}{2}\left|\log i\left(\frac{u+iv}{u-iv}\right)^p\right|. \tag{9}$$

Suppose first that $\alpha := \delta_4\left(\frac{u-iv}{-v+iu}\right)^\sigma$ is a root of unity for some $\sigma \in \{-1, 1\}$. Then

$$\left(\frac{u-iv}{-v+iu}\right)^\sigma = \frac{-2uv}{u^2+v^2} + \frac{\sigma(-u^2+v^2)}{u^2+v^2}i = \pm\alpha = \exp\left(\frac{2\pi i j}{n}\right),$$

for some integers j, n with $0 \leq j \leq n-1$. Therefore

$$\tan\left(\frac{2\pi j}{n}\right) = \frac{\sigma(-u^2+v^2)}{-2uv} \in \mathbb{Q} \text{ or } (u,v) = (0,0).$$

The latter case is excluded. Hence, by Lemma 4, $\frac{u^2-v^2}{2uv} \in \{0, 1, -1\}$. This implies that $|u| = |v|$, but this is excluded by the requirement that the solutions x, y of (1) are relatively prime, but $y > 126504$. Therefore α is not a root of unity.

Note that α is irrational, $|\alpha| = 1$, and it is a root of the polynomial $(u^2 + v^2)X^2 + 4\delta_4 uvX + (u^2 + v^2)$. Therefore $h(\alpha) = \frac{1}{2}\log y$.

Choose $l \in \mathbb{Z}$ such that $|p\log(i^{\delta_4}\frac{u+iv}{u-iv}) + 2l\pi i|$ is minimal, where logarithms have their principal values. Then $|2l| \leq p$. Consider the linear form in two logarithms ($\pi i = \log(-1)$)

$$\Lambda = 2|l|\pi i - p\log\alpha. \tag{10}$$

If $l = 0$ then by Liouville's inequality and Lemma 1 of [29],

$$|\Lambda| \geq |p\log\alpha| \geq |\log\alpha| \geq 2^{-2}\exp(-2h(\alpha)) \geq \exp(-8(\log 6)^3 h(\alpha)). \tag{11}$$

From (7) and (11) we obtain

$$\log 4 - \frac{p-1}{2}\log y \geq \log|\Lambda| \geq -4(\log 6)^3 \log y.$$

Hence $p \leq 47$. Thus we may assume without loss of generality that $l \neq 0$.

We apply Lemma 3 with $\sigma = \text{sign}(l), \alpha = \delta_4(\frac{u-iv}{-v+iu})^\sigma, b_1 = 2|l|$ and $b_2 = p$. Set $\lambda = 1.8$. We have $D = 1$ and $B = p$. By applying (7)-(10) and Lemma 3 we obtain

$$\log 4 - \frac{p-1}{2}\log y \geq \log|\Lambda| \geq -(13.16H^2 + 0.23)K - 2H - 2\log H - 0.004.$$

We have

$$\begin{aligned}
&15.37677 \leq K < 9.5028 + \frac{1}{2}\log y,\\
&0.008633 < t < 0.008634,\\
&0.155768 < T < 0.155769,\\
&H < \log p + 2.270616,\\
&\log y > 11.74803,
\end{aligned}$$

From the above inequalities we conclude that $p \leq 3803$. □

The following lemma gives a more precise description of the polynomial H_p.

Lemma 5. *The polynomial* $H_p(\pm q^k - \delta_4 v, v)$ *has degree* $p-1$ *and*

$$H_p(\pm q^k - \delta_4 v, v) = \pm\delta_8 2^{\frac{p-1}{2}} p v^{p-1} + q^k p \widehat{H}_p(v) + q^{k(p-1)},$$

where $\widehat{H}_p \in \mathbb{Z}[X]$ *has degree* $< p-1$. *The polynomial* $H_p(X,1) \in \mathbb{Z}[X]$ *is irreducible and*

$$H_p(X,1) = \prod_{\substack{k=0\\k\neq k_0}}^{p-1}\left(X - \tan\frac{(4k+3)\pi}{4p}\right),$$

where $k_0 = \left[\frac{p}{4}\right] \pmod 4$.

Proof. By definition we have

$$H_p(u,v) = \frac{G_p(u,v)}{u+\delta_4 v} = \frac{(1+i)(u+iv)^p - (1-i)(u-iv)^p}{2i(u+\delta_4 v)}. \tag{12}$$

Hence

$$H_p(\pm q^k - \delta_4 v, v) = \frac{(1+i)(\pm q^k + (i-\delta_4)v)^p - (1-i)(\pm q^k + (-i-\delta_4)v)^p}{\pm 2iq^k}.$$

Therefore the coefficient of v^p is $(1+i)(-\delta_4+i)^p + (1-i)(\delta_4+i)^p$. If $\delta_4 = 1$, then it equals $-2(-1+i)^{p-1} + 2(1+i)^{p-1} = -2(-4)^{\frac{p-1}{4}} + 2(-4)^{\frac{p-1}{4}} = 0$, since $p \equiv 1 \pmod 4$. If $\delta_4 = -1$, then it equals $(1+i)^{p+1} - (-1+i)^{p+1} = (-4)^{\frac{p+1}{4}} - (-4)^{\frac{p+1}{4}} = 0$. Similarly the coefficient of v^{p-1} is $\pm\frac{(1+i)(\delta_4-i)^{p-1} - (1-i)(\delta_4+i)^{p-1}}{2i}p = \pm\delta_8 2^{\frac{p-1}{2}}p$. It is easy to see that the constant is $q^{k(p-1)}$. The coefficient of v^t for $t = 1, \ldots, p-2$ is $\pm\binom{p}{t}(q^k)^{p-t-1}c_t$, where c_t is a power of 2. The irreducibility of $H_p(X,1)$ follows from the fact that $H_p(X-\delta_4, 1)$ satisfies Eisenstein's irreducibility criterion. The last statement of the lemma is a direct consequence of Lemma 4 from [27]. □

Remark. A conjecture, known as Schinzel's Hypothesis, says that if $P_1(X), ..., P_k(X) \in \mathbb{Z}[X]$ are irreducible polynomials such that no integer $l > 1$ divides $P_i(x)$ for all integers x for some $i \in \{1, \ldots, k\}$, then there exist infinitely many x such that $P_1(x), ..., P_k(x)$ are simultaneously prime. Since $H_p(\pm 1 - \delta_4 v, v)$ is irreducible having constant term ± 1, the Hypothesis implies that in case of $k = 0, m = 1$ there are infinitely many solutions of (1).

Lemma 6. *If there exists a* $k \in \{0, 1, \ldots, m\}$ *such that* (5) *or* (6) *has a solution* $(u,v) \in \mathbb{Z}^2$ *with* $\gcd(u,v) = 1$, *then either* $k = 0$ *or* $k = m, p \neq q$ *or* $(k = m-1, p = q)$.

Proof. Suppose $0 < k < m$. It follows from Lemma 5 that q divides $\pm\delta_8 2^{\frac{p-1}{2}} p v^{p-1}$. If $q \neq p$, we obtain that $q \mid v$ and $q \mid u$, which is a contradiction with $\gcd(u,v) = 1$. Thus $k = 0$ or $k = m$. If $p = q$, then from Lemma 5 and (5), (6) we get

$$\pm\delta_8 2^{\frac{p-1}{2}} v^{p-1} + p^k \widehat{H}_p(v) + p^{k(p-1)-1} = \pm p^{m-k-1}.$$

Therefore $k = 0$ or $k = m-1$. □

Now we are in the position to prove Theorem 1.

Proof of Theorem 1. By Lemma 6 we have that $k = 0, m-1$ or $k = m$. If $k = 0$, then $u + \delta_4 v = \pm 1$ and y is a sum of two consecutive squares. If $k = m-1$, then $p = q$. Hence $u + \delta_4 v = \pm p^{m-1}$ which implies that $y \geq \frac{p^{2(m-1)}}{2} \geq \frac{p^2}{2}$. From Theorem 2 we obtain that $p \leq 3089$. We recall that $H_p(u,v)$ is an irreducible polynomial of degree $p-1$. Thus we have only finitely many Thue equations (if $p > 3$)

$$H_p(u,v) = \pm p.$$

By a result of Thue [28] we know that for each p there are only finitely many integer solutions, which proves the statement.

Let $k = m$. Here we have $u + \delta_4 v = \pm q^m$ and $H_p(\pm q^m - \delta_4 v, v) = \pm 1$. If $q^m \leq 501$ then there are only finitely many solutions which are given in Lemma 1. We have computed an upper bound for p in Lemma 2 when $q^m \geq 503$. This leads to finitely many Thue equations

$$H_p(u,v) = \pm 1.$$

From Thue's result [28] follows that there are only finitely many integral solutions (u,v) for any fixed p, which implies the remaining part of the theorem. □

3. Fixed y

First we consider (1) with given y which is not a sum of two consecutive squares. Since $y = u^2 + v^2$ there are only finitely many possible pairs $(u,v) \in \mathbb{Z}^2$. Among these pairs we have to select those for which $u \pm v = \pm q^{m_0}$, for some prime q and for some integer m_0. Thus there are only finitely many pairs (q, m_0). The method of [27] makes it possible to compute (at least for moderate q and m_0) all solutions of $x^2 + q^{2m_0} = 2y^p$ even without knowing y. Let us consider the concrete example $y = 17$.

Theorem 3. *The only solution (m,p,q,x) in positive integers m,p,q,x with p and q odd primes of the equation $x^2 + q^{2m} = 2 \cdot 17^p$ is $(1,3,5,99)$.*

Proof. Note that 17 cannot be written as a sum of two consecutive squares. From $y = u^2 + v^2$ we obtain that q is 3 or 5 and $m = 1$. This implies that 17 does not divide x. We are left with the equations

$$x^2 + 3^2 = 2 \cdot 17^p,$$
$$x^2 + 5^2 = 2 \cdot 17^p.$$

From Lemma 1 we see that there is no solution with $q = 3, m = 1, y = 17$ and the only solution in case of the second equation is $(x,y,q,m,p) = (99,17,5,1,3)$. □

4. Fixed q

If m is small, then one can apply the method of [27] to obtain all solutions. Theorem 2 provides an upper bound for p in case $u + \delta_4 v = \pm q^m$. Therefore it is sufficient to resolve the Thue equations

$$H_p(u,v) = \pm 1$$

for primes less than the bound. In practice this is a difficult job but in some special cases there exist methods which work, see [5], [6], [7], [13]. Lemma 7 shows that we have a cyclotomic field in the background just as in [7]. Probably the result of the following lemma is in the literature, but we have not found a reference. We thank Peter Stevenhagen for the short proof.

Lemma 7. *For any positive integer M denote by ζ_M a primitive Mth root of unity. If α is a root of $H_p(X,1)$ for some odd prime p, then $\mathbb{Q}(\zeta_p + \overline{\zeta}_p) \subset \mathbb{Q}(\alpha) \cong \mathbb{Q}(\zeta_{4p} + \overline{\zeta}_{4p})$.*

Proof. Since $\tan z = \frac{1}{i}\frac{\exp(iz)-\exp(-iz)}{\exp(iz)+\exp(-iz)}$, we can write $\alpha = \tan(\frac{(4k+3)\pi}{4p})$ as

$$\frac{1}{i}\frac{\zeta_{8p}^{4k+3} - \zeta_{8p}^{-4k-3}}{\zeta_{8p}^{4k+3} + \zeta_{8p}^{-4k-3}} = -\zeta_4 \frac{\zeta_{4p}^{4k+3} - 1}{\zeta_{4p}^{4k+3} + 1} \in \mathbb{Q}(\zeta_{4p}).$$

Since it is invariant under complex conjugation, α is an element of $\mathbb{Q}(\zeta_{4p} + \overline{\zeta}_{4p})$. We also know that $[\mathbb{Q}(\zeta_{4p} + \overline{\zeta}_{4p}) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = p - 1$, thus $\mathbb{Q}(\zeta_{4p} + \overline{\zeta}_{4p}) \cong \mathbb{Q}(\alpha)$. The claimed inclusion follows from the fact that $\zeta_p + \overline{\zeta}_p$ can be expressed easily in terms of $\zeta_{4p} + \overline{\zeta}_{4p}$. □

It is important to remark that the Thue equations $H_p(u,v) = \pm 1$ do not depend on q. By combining the methods of composite fields [6] and non-fundamental units [13] for Thue equations we may rule out some cases completely. If the method applies it remains to consider the cases $u + \delta_4 v = \pm 1$ and $p = q$. If q is fixed one can follow a strategy to eliminate large primes p. Here we use the fact that when considering the Thue equation

$$H_p(u,v) = \pm 1. \tag{13}$$

we are looking for integer solutions (u,v) for which $u + \delta_4 v$ is a power of q. Let w be a positive integer relatively prime to q, then the set $S(q,w) = \{q^m \mod w : m \in \mathbb{N}\}$ has $\text{ord}_w(q)$ elements. Let

$$L(p,q,w) =$$
$$\{s \in \{0,1,\dots,\text{ord}_w(q)\} : H_p(q^s - \delta_4 v, v) = 1 \text{ has a solution modulo } w\}.$$

We search for numbers $w_1, \dots, w_N$ such that $\text{ord}_{w_1}(q) = \dots = \text{ord}_{w_N}(q) =: w$, say. Then

$$m_0 \mod w \in L(p,q,w_1) \cap \dots \cap L(p,q,w_N),$$

where $m_0 \mod w$ denotes the smallest non-negative integer congruent to m modulo w. Hopefully this will lead to some restrictions on m. As we saw before the special case $p = q$ leads to a Thue equation $H_p(u,v) = \pm p$ and the previously mentioned techniques may apply even for large primes. In case of $u + \delta_4 v = \pm 1$ one encounters a family of superelliptic equations $H_p(\pm 1 - \delta_4 v, v) = \pm q^m$. We will see that sometimes it is possible to solve these equations completely using congruence conditions only.

From now on we consider (1) with $q = 3$, that is

$$x^2 + 3^{2m} = 2y^p. \tag{14}$$

The equation $x^2 + 3 = y^n$ was completely resolved by Cohn [10]. Arif and Muriefah [2] found all solutions of the equation $x^2 + 3^{2m+1} = y^n$. There is one family of solutions, given by $(x,y,m,n) = (10 \cdot 3^{3t}, 7 \cdot 3^{2t}, 5 + 6t, 3)$. Luca [15] proved that all solutions of the equation $x^2 + 3^{2m} = y^n$ are of the form $x = 46 \cdot 3^{3t}, y = 13 \cdot 3^{2t}, m = 4 + 6t, n = 3$.

Remark. We note that equation (14) with odd powers of 3 is easily solvable. From $x^2 + 3^{2m+1} = 2y^p$ we get

$$4 \equiv 2y^p \pmod 8,$$

hence $p = 1$ which contradicts the assumption that p is prime.

Let us first treat the special case $p = q = 3$. By (4) and Lemma 2 we have

$$\begin{aligned} x &= F_3(u,v) = (u+v)(u^2 - 4uv + v^2), \\ 3^m &= G_3(u,v) = (u-v)(u^2 + 4uv + v^2). \end{aligned}$$

Therefore there exists an integer k with $0 \le k \le m$, such that

$$\begin{aligned} u - v &= \pm 3^k, \\ u^2 + 4uv + v^2 &= \pm 3^{m-k}. \end{aligned}$$

Hence we have

$$6v^2 \pm 6(3^k)v + 3^{2k} = \pm 3^{m-k}.$$

Both from $k = m$ and from $k = 0$ it follows easily that $k = m = 0$. This yields the solutions $(x, y) = (\pm 1, 1)$. If $k = m - 1 > 0$, then $3 \mid 2v^2 \pm 1$. Thus one has to resolve the system of equations

$$\begin{aligned} u - v &= -3^{m-1}, \\ u^2 + 4uv + v^2 &= -3. \end{aligned}$$

The latter equation has infinitely many solutions parametrized by

$$\begin{aligned} u &= \frac{-\varepsilon}{2}\left((2+\sqrt{3})^{t-1} + (2-\sqrt{3})^{t-1}\right), \\ v &= \frac{\varepsilon}{2}\left((2+\sqrt{3})^{t} + (2-\sqrt{3})^{t}\right), \end{aligned}$$

where $t \in \mathbb{N}, \varepsilon \in \{-1, 1\}$. Hence we get that

$$\frac{1}{2}\left((3+\sqrt{3})(2+\sqrt{3})^{t-1} + (3-\sqrt{3})(2-\sqrt{3})^{t-1}\right) = \pm 3^{m-1}. \tag{15}$$

The left-hand side of (15) is the explicit formula of the linear recursive sequence defined by $r_0 = r_1 = 3, r_t = 4r_{t-1} - r_{t-2}, t \geq 2$. One can easily check that

$$\begin{aligned} r_t \equiv 0 \pmod{27} &\Longleftrightarrow t \equiv 5 \text{ or } 14 \pmod{18}, \\ r_t \equiv 0 \pmod{17} &\Longleftrightarrow t \equiv 5 \text{ or } 14 \pmod{18}. \end{aligned}$$

Thus $m = 2$ or $m = 3$. If $m = 2, k = 1$, then we obtain the solution $(x, y) = (13, 5)$, if $m = 3, k = 2$, then we get $(x, y) = (545, 53)$. From now on we assume that $p > 3$.

As we mentioned, sometimes it is possible to handle the case $k = 0$ using congruence arguments only. In case of $q = 3$ it works.

Lemma 8. *In case of $q = 3$ there is no solution of* (5) *and* (6) *with $k = 0$.*

Proof. We give a proof for (5) which also works for (6). In case of (5) if $k = 0$, then $u = 1 - \delta_4 v$. Observe that by (12)

- if $v \equiv 0 \pmod 3$, then $H_p(1 - \delta_4 v, v) \equiv 1 \pmod 3$,
- if $v \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$, then $H_p(1 - \delta_4 v, v) \equiv 1 \pmod 3$,
- if $v \equiv 1 \pmod 3$ and $p \equiv 3 \pmod 4$, then $H_p(1 - \delta_4 v, v) \equiv \pm 1 \pmod 3$,
- if $v \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 4$, then $H_p(1 - \delta_4 v, v) \equiv \pm 1 \pmod 3$,
- if $v \equiv 2 \pmod 3$ and $p \equiv 3 \pmod 4$, then $H_p(1 - \delta_4 v, v) \equiv 1 \pmod 3$.

Thus $H_p(1 - \delta_4 v, v) \not\equiv 0 \pmod 3$. Therefore there is no $v \in \mathbb{Z}$ such that $H_p(1 - \delta_4 v, v) = 3^m$, as should be the case by (5) and (6). □

Finally we investigate the remaining case, that is $u + \delta_4 v = 3^m$. We remark that $u + \delta_4 v = -3^m$ is not possible because from (6) and Lemma 5 we obtain $-1 \equiv H_p(-3^m - \delta_4 v, v) \equiv 3^{k(p-1)} \equiv 1 \pmod p$.

Lemma 9. *If there is a coprime solution $(u, v) \in \mathbb{Z}^2$ of* (5) *with $q = 3, k = m$, then $p \equiv 5$ or $11 \pmod{24}$.*

Proof. In case of $k = m$ we have, by (5) and Lemma 5,

$$H_p(3^m - \delta_4 v, v) = \delta_8 2^{\frac{p-1}{2}} p v^{p-1} + 3^m p \widehat{H}_p(v) + 3^{m(p-1)} = 1. \tag{16}$$

Therefore

$$\delta_8 2^{\frac{p-1}{2}} p \equiv 1 \pmod 3$$

and we get that $p \equiv 1, 5, 7, 11 \pmod{24}$. Since by Lemma 1 the only solution of the equation $x^2 + 3^{2m} = 2y^p$ with $1 \leq m \leq 5$ is given by $(x, y, m, p) \in \{(79, 5, 1, 5), (545, 53, 3, 3)\}$, we may assume without loss of generality that $m \geq 6$. To get rid of the classes 1 and 7 we work modulo 243. If $p = 8t + 1$, then from (16) we have

$$2^{4t}(8t+1)v^{8t} \equiv 1 \pmod{243}.$$

It follows that $243|t$ and the first prime of the appropriate form is 3889 which is larger than the bound we have for p. If $p = 8t + 7$, then

$$-2^{4t+3}(8t+7)v^{8t+6} \equiv 1 \pmod{243}.$$

It follows that $t \equiv 60 \pmod{243}$ and it turns out that $p = 487$ is in this class, so we work modulo 3^6 to show that the smallest possible prime is larger than the bound we have for p. Here we have to resolve the case $m = 6$ using the method from [27]. This value of m is not too large so the method worked. We did not get any new solution. Thus $p \equiv 5$ or $11 \pmod{24}$. □

Theorem 4. *There exists no coprime integer solution* (x, y) *of* $x^2+3^{2m} = 2y^p$ *with* $m > 0$ *and* $p < 1000, p \equiv 5 \pmod{24}$ *or* $p \in \{131, 251, 491, 971\}$ *prime.*

Proof. To prove the theorem we resolve the Thue equations (13) for the given primes. In each case there is a small subfield, hence we can apply the method of [6]. We wrote a PARI [24] script to handle the computation. We note that if $p = 659$ or $p = 827$, then there is a degree 7 subfield, but the regulator is too large to get unconditional result, the same holds for $p = 419, 683, 947$, in these cases there is a degree 11 subfield. In the computation we followed the paper [6], but at the end we skipped the enumeration step. Instead we used the bound for $|x|$ given by the formula (34) at page 318. The summary of the computation is in Table 1. We obtained small bounds for $|u|$ in each case. It remains to find the integer solutions of the polynomial equations $H_p(u_0, v) = 1$ for the given primes with $|u_0| \leq X_3$. There is no solution for which $u + \delta v = 3^m, m > 0$, and the statement follows. □

Table 1: Summary of the computation (AMD64 Athlon 1.8GHz)

p	X_3	time	p	X_3	time	p	X_3	time	p	X_3	time	p	X_3	time	p	X_3	time
29	4	1s	149	2	7s	269	2	14s	461	2	22s	653	2	33s	797	2	45s
53	3	2s	173	2	6s	293	2	10s	491	2	25s	677	2	28s	821	2	56s
101	2	3s	197	2	7s	317	2	13s	509	2	23s	701	2	37s	941	2	62s
131	2	6s	251	2	14s	389	2	25s	557	2	27s	773	2	44s	971	2	75s

The Thue equations related to the remaining primes ($p < 1000$) were solved by G. Hanrot.

Theorem 5 (G. Hanrot)**.** *There exists no coprime integer solution* (x, y) *of* $x^2+3^{2m} = 2y^p$ *with* $m > 0$ *and* $p \in \{59, 83, 107, 179, 227, 347, 419, 443, 467, 563, 587, 659, 683, 827, 947\}$.

Proof. By combining the methods of composite fields [6] and non-fundamental units [13] all Thue equations were solved related to the given primes. The computations were done using PARI. Most of the computation time is the time for $p - 1$ LLL-reductions in dimension 3 on a lattice with integer entries of size about the square of the Baker bound. The numerical precision required in the worst case ($p = 587$) is 7700. The summary of the computation is in Table 2. We got small bounds for $|u|$ in each case. There is no solution for which $u + \delta v = 3^m, m > 0$, and the statement follows. □

We recall that Cohn [11] showed that the only positive integer solution of $x^2 + 1 = 2y^p$ is given by $x = y = 1$.

Theorem 6. *If the Diophantine equation* $x^2+3^{2m} = 2y^p$ *with* $m > 0$ *and* p *prime admits a coprime integer solution* (x, y)*, then* $(x, y, m, p) = (13, 5, 2, 3), (79, 5, 1, 5), (545, 53, 3, 3)$.

Table 2: Summary of the computation (AMD Opteron 2.6GHz)

p	X_3	time	p	X_3	time	p	X_3	time
59	47	2s	347	186	33m	587	279	248m
83	62	9s	419	216	67m	659	1	3s
107	74	23s	443	2	5s	683	2	7s
179	111	2m29s	467	233	102m	827	2	4s
227	134	6m13s	563	270	211m	947	2	10s

Proof. We will provide lower bounds for m which contradict the bound for p provided by Theorem 2. By Theorem 2 we have $p \leq 3803$ and by Lemma 9 we have $p \equiv 5$ or $11 \pmod{24}$. We compute the following sets for each prime p with $1000 \leq p \leq 3803, p \equiv 5$ or $11 \pmod{24}$:

$$\begin{aligned}
A5 &= L(p,3,242),\\
A16 &= L(p,3,136) \cap L(p,3,193) \cap L(p,3,320) \cap L(p,3,697),\\
A22 &= L(p,3,92) \cap L(p,3,134) \cap L(p,3,661),\\
A27 &= L(p,3,866) \cap L(p,3,1417),\\
A34 &= L(p,3,103) \cap L(p,3,307) \cap L(p,3,1021),\\
A39 &= L(p,3,169) \cap L(p,3,313),\\
A69 &= L(p,3,554) \cap L(p,3,611).
\end{aligned}$$

In case of $A5$ we have $\mathrm{ord}_{242}3 = 5$, hence this set contains those congruence classes modulo 5 for which (14) is solvable, similarly in case of the other sets. How can we use this information? Suppose it turns out that for a prime $A5 = \{0\}$ and $A16 = \{0\}$. Then we know that $m \equiv 0 \pmod{5 \cdot 16}$ and Theorem 2 implies $p \leq 1309$. If the prime is larger than this bound, then we have a contradiction. In Table 3 we included those primes for which we obtained a contradiction in this way. In the columns mod the numbers n are stated for which sets An were used for the given prime. It turned out that only 4 sets were needed. In case of $5, 22$ we have $m \geq 110, p \leq 1093$, in case of $16, 22$ we have $m \geq 176, p \leq 1093$ and in the case $16, 27$ we have $m \geq 432, p \leq 1009$. We could not exclude all primes using the previous argument, but there is an other way to use the computed sets. We can combine the available information by means of the Chinese remainder theorem. Let $CRT([a5, a16, a39], [5, 16, 39])$ be the smallest non-negative solution of the system of

Table 3: Excluding some primes using congruences.

p	mod	p	mod	p	mod	p	mod	p	mod
1013	16,27	1571	5,22	1973	16,22	2357	16,22	3011	5,22
1109	16,22	1613	16,22	1979	16,22	2459	16,22	3203	16,22
1181	16,22	1619	16,22	2003	16,22	2477	16,22	3221	16,22
1187	16,22	1667	16,22	2027	16,22	2531	5,22	3323	16,22
1229	16,22	1709	16,22	2069	16,22	2579	16,22	3347	16,22
1259	16,22	1733	16,22	2099	16,22	2693	16,22	3371	5,22
1277	16,22	1787	16,22	2141	16,22	2741	16,27	3413	16,22
1283	16,22	1811	5,22	2237	16,22	2861	16,22	3533	16,22
1307	16,22	1877	16,27	2243	16,22	2909	16,22	3677	16,22
1493	16,22	1931	5,22	2309	16,27	2957	16,22	3701	16,22
1523	16,22	1949	16,22	2333	16,22	2963	16,22		

Table 4: Excluding some primes using CRT.

p	r_m	CRT	p	r_m	CRT	p	r_m	CRT
1019	384	5,16,27	2267	448	5,16,69	3389	170	5,27,34
1061	176	5,16,39	2339	208	5,16,39	3461	116	5,16,39
1091	580	5,16,27	2381	44	5,27,34	3467	336	5,16,27
1163	586	5,27,34	2411	180	5,16,27	3491	850	5,27,34
1301	416	5,16,39	2549	320	5,16,27	3539	112	5,16,39
1427	270	5,27,34	2699	640	5,16,69	3557	176	5,16,39
1451	340	5,16,27	2789	204	5,27,34	3581	150	5,27,34
1499	112	5,16,39	2819	352	5,16,27	3659	112	5,16,39
1637	121	5,27,34	2837	131	5,27,34	3779	72	5,27,34
1901	304	5,16,39	2843	136	5,27,34	3797	416	5,16,39
1907	102	5,27,34	3083	340	5,27,34	3803	136	5,27,34
1997	170	5,27,34	3251	580	5,16,27			
2213	170	5,27,34	3299	64	5,16,39			

congruences

$$
\begin{aligned}
m &\equiv a5 \pmod 5\\
m &\equiv a16 \pmod{16}\\
m &\equiv a39 \pmod{39},
\end{aligned}
$$

where $a5 \in A5, a16 \in A16$ and $a39 \in A39$. Let r_m be the smallest non-zero element of the set $\{CRT([a5, a16, a39], [5, 16, 39]) : a5 \in A5, a16 \in A16, a39 \in A39\}$, In Table 4 we included the values of r_m and the numbers related to the sets $A5 - A69$. We see that $m \geq r_m$ in all cases. For example, if $p = 1019$ then $m \geq 384$, and Theorem 2 implies $p \leq 1009$, which is a contradiction. For $p = 2381$ we used $A5, A27$ and $A34$, given by $A5 = \{0, 1, 4\}, A27 = \{0, 14, 15, 17\}, A34 = \{0, 10\}$. Hence

$$
\begin{aligned}
&\{CRT([a5, a27, a34], [5, 27, 34]) : a5 \in A5, a27 \in A27, a34 \in A34\} =\\
&= \{0, 44, 204, 476, 486, 554, 690, 986, 1394, 1404, 1836, 1880, 1904,\\
&2040, 2390, 2526, 2754, 3230, 3240, 3444, 3716, 3740, 3876, 4226\}.
\end{aligned}
$$

The smallest non-zero element is 44 (which comes from $[a5, a27, a34] = [4, 17, 10]$), therefore $m \geq 44$ and $p \leq 1309$, a contradiction. In this way all remaining primes > 1000 can be handled. We are left with the primes $p < 1000, p \equiv 5$ or $11 \pmod{24}$ They are mentioned in Theorem 4 and in Theorem 5. □

Acknowledgement. The author wish to thank Guillaume Hanrot for the computations related to Theorem 5 and for giving some hints how to modify the PARI code, which was used in [7], to make the computations necessary for Theorem 4. Furthermore, we would like to thank Robert Tijdeman for his valuable remarks and suggestions, Peter Stevenhagen for the useful discussions on algebraic number theory, and for the proof of Lemma 7 and Kálmán Győry for calling our attention to Schinzel's Hypothesis.

REFERENCES

[1] S. A. Arif and F. S. A. Muriefah. On the Diophantine equation $x^2 + 2^k = y^n$. *Internat. J. Math. Math. Sci.*, 20(2):299–304, 1997.

[2] S. A. Arif and F. S. A. Muriefah. The Diophantine equation $x^2 + 3^m = y^n$. *Internat. J. Math. Math. Sci.*, 21(3):619–620, 1998.

[3] S. A. Arif and F S. A. Muriefah. On the Diophantine equation $x^2 + 2^k = y^n$. II. *Arab J. Math. Sci.*, 7(2):67–71, 2001.

[4] S. A. Arif and F. S. A. Muriefah. On the Diophantine equation $x^2 + q^{2k+1} = y^n$. *J. Number Theory*, 95(1):95–100, 2002.

[5] Yu. Bilu and G. Hanrot. Solving Thue equations of high degree. *J. Number Theory*, 60(2):373–392, 1996.

[6] Yu. Bilu and G. Hanrot. Thue equations with composite fields. *Acta Arith.*, 88(4):311–326, 1999.

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

[8] Y. Bugeaud. On the Diophantine equation $x^2 - p^m = \pm y^n$. *Acta Arith.*, 80(3):213–223, 1997.

[9] J. H. E. Cohn. The Diophantine equation $x^2 + 2^k = y^n$. *Arch. Math. (Basel)*, 59(4):341–344, 1992.

[10] J. H. E. Cohn. The Diophantine equation $x^2 + 3 = y^n$. *Glasgow Math. J.*, 35(2):203–206, 1993.

[11] J. H. E. Cohn. Perfect Pell powers. *Glasgow Math. J.*, 38(1):19–20, 1996.

[12] J. H. E. Cohn. The Diophantine equation $x^2 + 2^k = y^n$. II. *Int. J. Math. Math. Sci.*, 22(3):459–462, 1999.

[13] G. Hanrot. Solving Thue equations without the full unit group. *Math. Comp.*, 69(229):395–405, 2000.

[14] Maohua Le. On the Diophantine equation $x^2 + p^2 = y^n$. *Publ. Math. Debrecen*, 63(1-2):67–78, 2003.

[15] F. Luca. On a Diophantine equation. *Bull. Austral. Math. Soc.*, 61(2):241–246, 2000.

[16] F. Luca. On the equation $x^2 + 2^a \cdot 3^b = y^n$. *Int. J. Math. Math. Sci.*, 29(4):239–244, 2002.

[17] M. Mignotte. On the Diophantine equation $D_1x^2 + D_2^m = 4y^n$. *Portugal. Math.*, 54(4):457–460, 1997.

[18] F. S. A. Muriefah. On the Diophantine equation $px^2 + 3^n = y^p$. *Tamkang J. Math.*, 31(1):79–84, 2000.

[19] F. S. A. Muriefah. On the Diophantine equation $Ax^2 + 2^{2m} = y^n$. *Int. J. Math. Math. Sci.*, 25(6):373–381, 2001.

[20] F. S. A. Muriefah and S. A. Arif. On a Diophantine equation. *Bull. Austral. Math. Soc.*, 57(2):189–198, 1998.

[21] F. S. A. Muriefah and S. A. Arif. The Diophantine equation $x^2 + 5^{2k+1} = y^n$. *Indian J. Pure Appl. Math.*, 30(3):229–231, 1999.

[22] F. S. A. Muriefah and S. A. Arif. The Diophantine equation $x^2 + q^{2k} = y^n$. *Arab. J. Sci. Eng. Sect. A Sci.*, 26(1):53–62, 2001.

[23] I. Niven. *Irrational numbers*. The Carus Mathematical Monographs, No. 11. The Mathematical Association of America. Distributed by John Wiley and Sons, Inc., New York, N.Y., 1956.

[24] The PARI Group, Bordeaux. *PARI/GP, version* `2.2.8`, 2004. available from http://pari.math.u-bordeaux.fr/.

[25] I. Pink. On the Diophantine equation $x^2 + (p_1^{z_1} \dots p_s^{z_s})^2 = 2y^n$. *Publ. Math. Debrecen*, 65(1-2):205–213, 2004.

[26] I. Pink and Sz. Tengely. Full powers in arithmetic progressions. *Publ. Math. Debrecen*, 57(3-4):535–545, 2000.

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

[28] A. Thue. Über Annäherungswerte algebraischer Zahlen. *J. Reine Angew Math.*, 135:284–305, 1909.

[29] P. M. Voutier. Primitive divisors of Lucas and Lehmer sequences. II. *J. Théor. Nombres Bordeaux*, 8(2):251–274, 1996.

MATHEMATICAL INSTITUTE
UNIVERSITY OF DERECEN
P.O.BOX 12
4010 DEBRECEN
HUNGARY
E-mail address: `tengely@math.klte.hu`