ON THE DIOPHANTINE EQUATION $x^2 + a^2 = 2y^p$

SZ. TENGELY

Dedicated to Professor Robert Tijdeman on the occasion of his 60th birthday

1. Introduction

The title equation is a special case of

$$Ax^p + By^q = Cz^r.$$

Darmon and Granville [20] wrote down a parametrization for each case when $1/p + 1/q + 1/r > 1$ and $A = B = C = 1$. Beukers [9] showed that for any nonzero integers A, B, C, p, q, r for which $1/p + 1/q + 1/r > 1$ all solutions of $Ax^p + By^q = Cz^r$ can be obtained from a finite number of parametrized solutions. The theory of binary quadratic forms (see e.g. [31], Chapter 14) applies to the case $\{p, q, r\} = \{2, 2, k\}$ and a set of parametrizations can be found easily. We will make use of the fact, that in case of the title equation the parametrization is reducible.

It follows from Schinzel and Tijdeman [38] that for given non-zero integers A, B, C the equation $Ax^2 + B = Cy^n$ has only a finite number of integer solutions $x, y, n > 2$, which can be effectively determined. For special values of A, B and C this equation was investigated by several authors see e.g. [8], [16], [19], [22], [23], [25], [26],[34], [40] and the references given there. The equation

$$x^2 + 7 = y^n$$

is still unsolved. The known solutions are obtained for $x = \pm 1, \pm 3, \pm 5, \pm 11, \pm 181$. We note that using tools from arithmetic algebraic geometry recently Siksek and Cremona [39] have proved that if (x, y, n) is any unknown solution of this equation then $10^8 < n < 6.6 \times 10^{15}$.

There are many results concerning the more general Diophantine equation

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

where p_i is prime for all i and z_i is an unknown non-negative integer, see e.g. [1], [2], [3], [4], [5], [6], [7], [13], [15], [18], [27], [28], [29], [32], [33], [37]. Here the elegant result of Bilu, Hanrot and Voutier [12] on the existence of primitive divisors of Lucas and Lehmer numbers has turned out to be a very powerful tool. In [37] 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.

2000 *Mathematics Subject Classification.* Primary 11D41; Secondary 11D25.
Key words and phrases. Diophantine equations.

In [24] Ljunggren proved that if p is a given prime such that p^2-1 is exactly divisible by an odd power of 2, then the equation $x^2+p^2=y^n$ has only a finite number of solutions in x, y and n with $n>1$. He provided a method to find all the solutions in this case.

The equation $x^2+1=2y^n$ was solved by Cohn [17]. Pink and Tengely [36] considered the title equation and they gave an upper bound for the exponent n depending only on a, and they completely resolved the equation with $1 \le a \le 1000$ and $3 \le n \le 80$. The theorems in the present paper provide a method to resolve the equation $x^2+a^2=2y^n$ in integers $n>2, x, y$ for any fixed a. In particular we compute all solutions for odd a with $3 \le a \le 501$.

2. Results

Consider the Diophantine equation

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

where a is a given positive integer and $x, y \in \mathbb{N}$ such that $\gcd(x,y)=1$ and $p \ge 3$ a prime. Put

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

After having read the paper [36], Bugeaud suggested to use linear forms in only two logarithms in order to improve the bound for the exponent. Following this approach we get a far better bound than Pink and Tengely did in [36], that is, than $p < 2^{91}5^{27}a^{10}$.

Theorem 1. *If (x,y,p) is a solution of $x^2+a^2=2y^p$ with $y>50000$ then*

$$p \le \max\left\{\frac{4\log a}{\log 50000}, 9511\right\}.$$

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

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

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

In the proof we will use the following result of Mignotte [4,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 1. *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

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

Then

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

We shall use the following statement in the proof of Theorem 1. The result can be found as Corollary 3.12 at p. 41 of [35].

Lemma 2. *If $\Theta = 2\pi r$ for some rational number r, then the only rational values of the tangent and the cotangent functions at Θ can be $0, \pm 1$.*

Proof of Theorem 1. Without loss of generality we assume that $p > 2000, y > 50000$, and $y^p > a^4$. Then, by (1), we have $x^2 > y^p$ and $x > a^2$. We compute an upper bound for $|\frac{x+ai}{x-ai} - 1|$:

$$\left|\frac{x+ai}{x-ai} - 1\right| = \frac{2a}{\sqrt{x^2+a^2}} = \frac{2}{\sqrt{\frac{x^2}{a^2}+1}} < \frac{2}{\sqrt{x+1}} < \frac{2}{y^{p/4}}. \tag{3}$$

We have

$$\frac{x+ai}{x-ai} = \frac{(1+i)(u+iv)^p}{(1-i)(u-iv)^p} = i\frac{(u+iv)^p}{(u-iv)^p}.$$

If $\left|i\frac{(u+iv)^p}{(u-iv)^p} - 1\right| > \frac{1}{3}$ then $p \le \frac{4\log 6}{\log 50000} < 2000$, a contradiction. Thus $\left|i\frac{(u+iv)^p}{(u-iv)^p} - 1\right| \le \frac{1}{3}$. Since $|\log z| \le 2|z-1|$ for $|z-1| \le \frac{1}{3}$, we obtain

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

Consider the corresponding linear form in two logarithms ($\pi i = \log(-1)$)

$$\Lambda = 2k\sigma\pi i - p\log\left(\delta\left(\frac{u-iv}{-v+iu}\right)^{\sigma}\right),$$

where logarithms have their principal values, $|2k| \le p$ and $\sigma = \mathrm{sign}(k)$. We apply Lemma 1 with $\alpha = \delta(\frac{u-iv}{-v+iu})^\sigma, b_1 = 2k\sigma$ and $b_2 = p$.

Suppose α is a root of unity. Then

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

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

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

Hence, by Lemma 2, $\frac{(u^2-v^2)}{2uv} \in \{0, 1, -1\}$. This implies that $uv = 0$ or $|u| = |v|$, but this is excluded by the requirement that the solutions x, y of (1) are relatively prime and that $y > 50000$. Therefore α is not a root of unity.

Note that α is irrational, $|\alpha| = 1$, and it is root of the polynomial $(u^2+v^2)X^2 + 4\delta uvX + (u^2+v^2)$. Therefore $h(\alpha) = \frac{1}{2}\log y$. Set $\lambda = 1.8$. We have $D = 1$ and $B = p$ and $K \le 9.503 + \frac{1}{2}\log y$. We also have

$$H \le \log p + \log\left(0.53 + \frac{1}{19+\log y}\right) + \frac{4.28}{19+\log y} + 4.6. \tag{4}$$

By applying Lemma 1 we obtain

$$\log 4 - \frac{p}{4}\log y \ge \log|\Lambda| \ge -(13.16H^2 + 0.23)K - 2H - 2\log H - 0.003.$$

From the above inequalities we conclude that $p \le 9511$. Thus we obtain the bound $p \le \max\left\{\frac{4\log a}{\log 50000}, 9511\right\}$. □

Remark. We also have in place of (3) that

$$\left|\frac{x+ai}{x-ai} - 1\right| \le \frac{\sqrt{2}a}{y^{p/2}}.$$

Hence

$$\log 2\sqrt{2}a - \frac{p}{2}\log y \ge \log|\Lambda| \ge -(13.16H^2 + 0.23)K - 2H - 2\log H - 0.003. \tag{5}$$

This yields by (4) an upper bound $C(a, y)$ for p depending only on a and y.

Theorem 2 gives us a tool to resolve Diophantine equations of type (1) for given a completely.

Theorem 2. *Let*

$$\mathcal{A}(C) = \bigcup_{p \le C}\left\{\tan\frac{(4k+3)\pi}{4p} : 0 \le k \le p-1\right\},$$

$$T = \begin{cases} \mathrm{lcm}(\mathrm{ord}_u(v), \mathrm{ord}_v(u)) \text{ } \textit{if } \min\{|u|, |v|\} \ge 2, \\ \max\{|u|, |v|\} \text{ } \textit{otherwise}, \end{cases}$$

and δ is defined by (2). If (x, y, p) is a solution of $x^2 + a^2 = 2y^p$ such that $\gcd(x, y) = 1$, then there exist integers u, v satisfying $(u, v, p) \in S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5$ where

$$\begin{aligned}
S_1 &= \{(u,v,p) : u + \delta v = a_0, a_0 \neq a, a_0 | a, p | a - a_0, G_p(-\delta v + a_0, v) = a\}, \\
S_2 &= \{(u,v,p) : u + \delta v = a, p \in \{3,5,7\}, G_p(-\delta v + a, v) = a\}, \\
S_3 &= \left\{(u,v,p) : u + \delta v = a, u^2 + v^2 \leq 50000, 11 \leq p \leq C(a, u^2 + v^2), p \equiv \pm 1 \bmod T\right\}, \\
S_4 &= \left\{(u,v,p) : u + \delta v = a, |u| > 223, |v| = 1, 11 \leq p \leq C(a, 50000), p \equiv \pm 1 \bmod T\right\}, \\
S_5 &= \Big\{(u,v,p) : u + \delta v = a, u^2 + v^2 > 50000, |v| \geq 2, 11 \leq p \leq C(a, 50000), \\
&\quad \frac{a}{v} \text{ is a convergent of } \beta + \delta \text{ for some } \beta \in \mathcal{A}(C(a, 50000))\Big\}.
\end{aligned}$$

To prove Theorem 2 we need the following lemmas.

Lemma 3. *If l is an odd positive integer, then*

$$\begin{aligned}
(u - \delta v) &\mid F_l(u, v), \\
(u + \delta v) &\mid G_l(u, v).
\end{aligned}$$

Proof. If $l \equiv 1 \pmod 4$ then

$$F_l(u, u) = \frac{u^l}{2}((1 + i)^{l+1} + (1 - i)^{l+1}) = 0,$$

and also

$$G_l(u, -u) = \frac{u^l}{2i}((1 - i)^{l-1} - (1 + i)^{l-1}) = 0.$$

The proof of the other case is similar. □

Lemma 4. *We have*

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

Proof. By definition $G_p(X, 1) = \Im((1 + i)(X + i)^p)$. We have

$$\begin{aligned}
2i \left(\cos \frac{(4k + 3)\pi}{4p}\right)^p G_p(\tan \frac{(4k + 3)\pi}{4p}, 1) &= \\
= i^p(1 + i)(-1)^k \left(\exp\left(\frac{-3i\pi}{4}\right) - i \exp\left(\frac{3i\pi}{4}\right)\right) &= 0.
\end{aligned}$$

Hence $G_p(\tan \frac{(4k+3)\pi}{4p}, 1) = 0$ for $0 \leq k \leq p - 1$. Since $G_p(X, 1)$ has degree p and G_p is monic, the lemma follows. □

Proof of Theorem 2. We have seen that $a = \Im((1+i)(u+iv)^p) =: G_p(u,v)$. Hence Lemma 3 implies that $u + \delta v | a$, that is, there exists an integer a_0 such that $a_0 | a$ and $u + \delta v = a_0$. Define a function $s : \mathbb{N} \to \{\pm 1\}$ as follows:

$$s(k) = \begin{cases} 1 \text{ if } k \equiv 0, 1 \pmod 4, \\ -1 \text{ if } k \equiv 2, 3 \pmod 4. \end{cases}$$

It follows that

$$a = G_p(-\delta v + a_0, v) = \sum_{k=0}^{p} s(k) \binom{p}{k} (-\delta v + a_0)^{p-k} v^k,$$

hence

$$a \equiv (-\delta v + a_0)^p + \delta v^p \equiv a_0 \pmod p.$$

If $a_0 \neq a$ then it remains to solve the polynomial equations

$$G_p(-\delta v + a_0, v) = a, \quad \text{for } a_0 | a, a_0 \neq a \text{ and } p | a - a_0. \tag{6}$$

That is the first instance mentioned in Theorem 2.

From now on we assume that $a_0 = a = u + \delta v$. We claim $p \equiv \pm 1 \bmod T$. We note that

$$1 \equiv \frac{G_p(u,v)}{u + \delta v} \equiv u^{p-1} + (p - \delta) u^{p-2} v \bmod v^2,$$
$$1 \equiv \frac{G_p(u,v)}{u + \delta v} \equiv v^{p-1} + (p - \delta) v^{p-2} u \bmod u^2.$$

Suppose that $|u| = 1$. Then either $v = 0$ or $(p - \delta)v \equiv 0 \bmod v^2$, that is $p \equiv \delta \bmod v$ and the claim is proved. The case $|v| = 1$ is similar. Now assume that $\min\{|u|, |v|\} \geq 2$. In this case we obtain that

$$u^{p-1} \equiv 1 \bmod v,$$
$$v^{p-1} \equiv 1 \bmod u,$$

and therefore $\mathrm{ord}_v(u) | p - 1$ and $\mathrm{ord}_u(v) | p - 1$. Hence

$$T = \mathrm{lcm}(\mathrm{ord}_u(v), \mathrm{ord}_v(u)) | p - 1.$$

If $y \leq 50000$ then we have $|u| \leq 224, |v| \leq 224$, therefore a belongs to the finite set $\{u + \delta v : |u| \leq 224, |v| \leq 224, u^2 + v^2 \leq 50000\}$. For all possible pairs (u, v) we have $p \leq C(a, u^2 + v^2)$ and $p \equiv \pm 1 \bmod T$. Thus $(u, v, p) \in S_3$.

Consider the case $y > 50000$. Let $\beta_i, i = 1, \ldots, p$ be the roots of the polynomial $G_p(X, 1)$, such that $\beta_1 < \beta_2 < \ldots < \beta_p$. Let $\gamma_i = u - \beta_i v$, and $\gamma_{i_1} = \min_i |\gamma_i|$. From Lemma 3 it follows that there is an index i_0 such that $|\beta_{i_0}| = 1$. From $G_p(u, v) = a$ we obtain

$$\prod_{\substack{i=1 \\ i \neq i_0}}^{p} (u - \beta_i v) = 1. \tag{7}$$

Using the mean-value theorem one can easily prove that

$$\left|\tan\frac{(4k_1+3)\pi}{4p} - \tan\frac{(4k_2+3)\pi}{4p}\right| \geq |k_1-k_2|\frac{\pi}{p}.$$

Hence, by Lemma 4

$$|\gamma_i - \gamma_j| = |(\beta_i - \beta_j)v| \geq \frac{|i-j|\pi}{p}|v|.$$

If γ_{i_1} and γ_{i_1+k} have the same sign then we obtain that

$$|\gamma_{i_1+k}| \geq \frac{|k|\pi}{p}|v|,$$

otherwise

$$|\gamma_{i_1+k}| \geq \frac{(2|k|-1)\pi}{2p}|v|.$$

Hence, from (7) we get

$$1 = \prod_{\substack{i=1\\ i\neq i_0}}^{p} |u-\beta_i v| = \prod_{\substack{i=1\\ i\neq i_0}}^{p} |\gamma_i| \geq (p-2)!|\gamma_{i_1}|\left(\frac{\pi|v|}{2p}\right)^{p-2}.$$

If $|\gamma_{i_1}| < \frac{1}{2|v|}$, then $|\frac{a}{v} - (\beta_{i_1}+\delta)| < \frac{1}{2v^2}$, hence $\frac{a}{v}$ is a convergent of $\beta_{i_1}+\delta$. If $|\gamma_{i_1}| \geq \frac{1}{2|v|}$, then

$$1 \geq \frac{1}{2|v|}(p-2)!\left(\frac{\pi|v|}{2p}\right)^{p-2} > \frac{\sqrt{2\pi}}{2|v|}\left(\frac{\pi(p-2)|v|}{2ep}\right)^{p-2}, \tag{8}$$

where we used the inequality $(p-2)! > \sqrt{2\pi}(\frac{p-2}{e})^{p-2}$. From (8) it follows that

$$|v| \leq \left(\frac{\sqrt{2}}{\sqrt{\pi}}\left(\frac{2e}{\pi}+\frac{4e}{\pi(p-2)}\right)\right)^{\frac{1}{p-3}}\left(\frac{2e}{\pi}+\frac{4e}{\pi(p-2)}\right),$$

it is easy to see that the right-hand side is a strictly decreasing function of p and that $|v| < 2$ for $p \geq 19$. We get the same conclusion for $p \in \{11,13,17\}$ from (8). Now, if $p \in \{3,5,7\}$, then it remains to solve $G_p(-\delta v + a, v) = a$. If $|v| < 2$, then we have to check only the cases $v = \pm 1$, because in case of $v = 0$ we do not obtain any relatively prime solution. Hence $(u,v,p) \in S_4$. If $|v| > 2$, then $|\gamma_{i_1}| < \frac{1}{2|v|}$, that is $\frac{a}{v}$ is a convergent of $\beta_{i_1}+\delta$. We conclude that $(u,v,p) \in S_5$, and the theorem is proved. □

2.1. **The Diophantine equation $x^2+a^2=y^p$.** We recall that Ljunggren proved that if a is a given prime such that a^2-1 is exactly divisible by an odd power of 2, then the equation $x^2+a^2=y^n$ has only a finite number of solutions in x, y and n with $n>1$. He provided a method to find all the solutions in this case. We shall only require that $a \neq 0$. In this case we get the following parametrization

$$\begin{aligned} x &= \Re((u+iv)^p) =: f_p(u,v), \\ a &= \Im((u+iv)^p) =: g_p(u,v). \end{aligned}$$

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

Theorem 3. *If (x,y,p) is a solution of $x^2+a^2=y^p$ with $y>50000$ then*

$$p \leq \max\left\{\frac{4\log a}{\log 50000}, 9511\right\}.$$

Proof. The proof goes in the same way as that of Theorem 1, so we indicate a few steps only. Without loss of generality we assume that $p>2000, y>50000$, and $y^p>a^4$. The inequality $y^p>a^4$ implies that $x^2>y^p-y^{p/2}\geq(y^{p/2}-1)^2$, thus $x+1>y^{p/2}$. Hence we have

$$\left|\frac{x+ai}{x-ai}-1\right| = \frac{2a}{\sqrt{x^2+a^2}} < \frac{2}{y^{p/4}}. \tag{9}$$

Consider the corresponding linear form in two logarithms

$$\Lambda = 2k\sigma\pi i - p\log\left(\left(\frac{u-iv}{u+iv}\right)^{\sigma}\right),$$

where logarithms have their principal values, $|2k|\leq p$ and $\sigma=\mathrm{sign}(k)$. We apply Lemma 1 with $\alpha=\delta(\frac{u-iv}{u+iv})^{\sigma}, b_1=2k\sigma$ and $b_2=p$. As in the proof of Theorem 1 we find that α is not a root of unity. It is a root of the polynomial $(u^2+v^2)X^2-2(u^2-v^2)X+(u^2+v^2)$. Therefore $h(\alpha)=\frac{1}{2}\log y$. Set $\lambda=1.8$. We have $D=1$ and $B=p$ and $K\leq 9.503+\frac{1}{2}\log y$. By applying Lemma 1 we obtain

$$\log 4-\frac{p}{4}\log y \geq \log|\Lambda| \geq -(13.16H^2+0.23)K-2H-2\log H-0.003.$$

From the above inequalities we conclude that $p\leq 9511$. Thus we obtain the bound $p\leq\max\left\{\frac{4\log a}{\log 50000}, 9511\right\}$. □

Remark. We also have in place of (9) that

$$\left|\frac{x+ai}{x-ai}-1\right| \leq \frac{2a}{y^{p/2}}.$$

Hence

$$\log 4a-\frac{p}{2}\log y \geq \log|\Lambda| \geq -(13.16H^2+0.23)K-2H-2\log H-0.003. \tag{10}$$

We have the bound (4) for H, this yields an upper bound $C_1(a,y)$ for p depending only on a and y, which is decreasing with respect to y.

Theorem 4. *If (x, y, p) is a solution of $x^2 + a^2 = y^p$ such that $\gcd(x, y) = 1, a \neq 0$, then there exist integers u, v satisfying $(u, v, p) \in S_1 \cup S_2 \cup S_3$ where*

$$\begin{aligned} S_1 &= \{(u, v, p) : v = a_0, a_0 \neq \delta a, a_0 | a, p | a - \delta a_0, g_p(u, a_0) = a\}, \\ S_2 &= \left\{(u, v, p) : v = \delta a, u^2 + a^2 \leq 50000, 3 \leq p \leq C(a, u^2 + a^2), a^{p-1} \equiv 1 \bmod u^2\right\}, \\ S_3 &= \left\{(u, v, p) : v = \delta a, |u| \leq \cot\left(\frac{\pi}{p}\right) a + 1 \text{ and } 3 \leq p \leq C_1(a, 50000)\right\}. \end{aligned}$$

We have similar lemmas as we applied to prove Theorem 2.

Lemma 5. *If l is an odd positive integer, then*

$$\begin{aligned} u &\mid f_l(u, v), \\ v &\mid g_l(u, v). \end{aligned}$$

Proof. By definition $g_l(u, v) = \Im((u+iv)^l) = \frac{(u+iv)^l - (u-iv)^l}{2i}$, therefore $g_l(u, 0) = 0$. Similarly for f_p. □

Lemma 6. *We have*

$$g_p(X, 1) = p \prod_{k=1}^{p-1} \left(X - \cot \frac{k\pi}{p}\right).$$

Proof. We have

$$2i \left(\sin \frac{k\pi}{p}\right)^p g_p(\cot \frac{k\pi}{p}, 1) = \exp(ik\pi) - \exp(-ik\pi) = 0.$$

Hence $g_p(\cot \frac{k\pi}{p}, 1) = 0$ for $1 \leq k \leq p - 1$. □

In the proof of Theorem 1 it is clear from (7) that there exists an index j such that $|u - \beta_j v| \leq 1$. Since $u + \delta v = a$ it follows that

$$|v| \leq \frac{a + 1}{|\beta_j + \delta|}.$$

The denominator can be quite small, therefore we do not get a useful bound for $|v|$. In the present case we are lucky, we can use the equation

$$p \prod_{k=1}^{p-1} \left(u - \delta a \cot \frac{k\pi}{p}\right) = 1 \tag{11}$$

to get a bound for $|u|$ and resolve $x^2 + a^2 = y^p$ completely.

Proof of Theorem 4. From Lemma 5 we obtain that $v \mid a$, therefore there exists an integer a_0 such that $a_0 \mid a$ and $a_0 = v$. Thus

$$g_p(u, a_0) = a,$$

which implies that $p \mid a - \delta a_0$. If $a_0 \neq \delta a$ then we get $(u, v, p) \in S_1$. Consider the case $a_0 = \delta a$. If $y \leq 50000$ then we have $u^2 + a^2 \leq 50000$ and (10) provides

a bound $C_1(a, u^2+a^2)$ for p. Now we prove the congruence condition on p using the equation $g_p(u, \delta a) = a$. Hence, by $\delta^2 = 1$,

$$1 = a^{-1} g_p(u, \delta a) = \sum_{k=1}^{\frac{p+1}{2}} s(2k-1) \binom{p}{2k-1} u^{p-2k+1} \delta a^{2k-2}.$$

This implies that

$$s(p) \delta a^{p-1} \equiv 1 \bmod u^2.$$

Thus $(u, v, p) \in S_2$. If $y > 50000$ then from (10) we obtain that $p < C_1(a, 50000)$. By (11) there is an integer $1 \le j \le p-1$ such that $|u - \delta a \cot \frac{j\pi}{p}| < 1$. Hence

$$|u| < a \cot \frac{\pi}{p} + 1,$$

so $(u, v, p) \in S_3$. □

Remark. We note that the method that we apply in this paper works for some equations of the type

$$x^2 + a^2 = cy^p$$

with $a \neq 0, c \neq 1, 2$ an even integer, as well.

3. Numerical results

3.1. **Resolution of** (1) **with** $a \in \{3, 5, \ldots, 501\}$**.** Applying Theorem 2 we obtain the following result.

Corollary 1. *Let a be an odd integer with $3 \le a \le 501$. If $(x, y) \in \mathbb{N}^2$ is a positive solution of $x^2 + a^2 = 2y^p$ such that $x \ge a^2, \gcd(x, y) = 1$ then*

$$(a, x, y, p) \in \big\{(3, 79, 5, 5), (5, 99, 17, 3), (19, 5291, 241, 3), (71, 275561, 3361, 3)$$
$$(99, 27607, 725, 3), (265, 14325849, 46817, 3), (369, 1432283, 10085, 3)\big\}.$$

Proof. Finding the elements of the five sets in Theorem 2 provides the solutions of (1). We describe successively how to find the elements of these sets.

I. For a given a one has to resolve (6), that is several polynomial equations. One can perform this job either by factoring the polynomial or by testing the divisors of the constant term of the polynomial. Nowadays the computer algebra programs contain procedures to find all integral solutions of polynomial equations. We used Magma to do so. The total CPU time for step I was about 44 minutes. For example when $a = 249$ then $a_0 \in \{-249, -83, -3, -1, 1, 3, 83\}$, therefore $p \in \{3, 5, 7, 31, 41, 83\}$. There is only one solution: $(x, y, p) = (307, 5, 7)$. It took 0.4 sec to solve this case completely. In the list only the last solution is derived from this part.

II. The cases $p = 3, p = 5$ and $p = 7$. If $p = 3$ then we have only to solve quadratic equations of the form

$$6v^2 + 6av + a^2 - 1 = 0.$$

We obtained the following solutions indicated in the list:
$(5, 99, 17, 3), (19, 5291, 241, 3), (71, 275561, 3361, 3), (265, 14325849, 46817, 3)$.
If $p = 5$ then we get the Thue equation

$$\frac{G_5(X, Y)}{X + Y} = X^4 + 4X^3Y - 14X^2Y^2 + 4XY^3 + Y^4 = 1$$

which has only the solutions $(\pm 1, \pm 2), (\pm 2, \pm 1), (\pm 1, 0), (0, \pm 1)$. Therefore the solutions of (1) with $p = 5$ and $u+v = a$ are given by $(a, x, y) \in \{(1, 1, 1), (3, 79, 5)\}$. If $p = 7$ then the corresponding Thue equation has only trivial solutions, hence the only solution of (1) with $p = 7, u - v = a$ is $(a, x, y) = (1, 1, 1)$. The total CPU time for step II was about 1.8 seconds.

III. If (u, v, p) belongs to S_3, then $|u| \leq 224$ and $|v| \leq 224$. Since we are interested only in relatively prime solutions of (1), we have to check only those pairs (u, v) for which $u + \delta v = a, \gcd(u, v) = 1, 2 \nmid u - v$ and $u^2 + v^2 \leq 50000$. For such a pair (u, v) one can compute T easily, and from (5) one gets $C(a, u^2 + v^2)$. So we obtain the set S_3. It remains to check which triples yield a solution of (1). To do so we compute $y = u^2 + v^2$ and we examine whether $2y^p - a^2$ is a square. This last step can be done efficiently, see [14], pp. 39-41. We used the appropriate procedure of Magma. We did not obtain any solution in this case with $p \geq 11$. The total CPU time for step III was about 24.4 hours.

IV. In case of S_4 and S_5 we have a common bound for p which can be obtained from (5). It turns out that this bound is 4079. Since $v = \pm 1$ we have $y = a^2 \pm 2a + 2$. We check whether $2(a^2 \pm 2a + 2)^p - a^2$ is a square for all primes $p \leq 4079, p \equiv \pm 1 \bmod T$. There is no solution. The total CPU time was about 1.9 minutes.

V. To get S_5 we have to compute approximate values of some real numbers of the form

$$\tan \frac{(4k + 3)\pi}{4p}.$$

We note that we do not need very high precision, since the numerators of the convergents are bounded by a, in our case at most 501. We computed all convergents of the real numbers contained in $\mathcal{A}(C(a, 50000))$ with numerator at most 501. From the triples (u, v, p) of S_5 we got the solutions of (1) as in the previous cases. For example, for $a = 501$ we obtained several convergents, one of them being

$$\frac{501}{45848} \approx 0.010927412319,$$

which is a convergent of

$$\tan \frac{(4 \cdot 993 + 3)\pi}{4 \cdot 4003} \approx 0.010927412156.$$

We did not get any solution of (1) from this part. The total CPU time for step IV was about 3.36 days. □

Applying Theorem 4 we obtain the following result in case y^p has coefficient 1.

Corollary 2. *Let a be an odd integer with $3 \leq a \leq 501$. If $(x,y) \in \mathbb{N}^2$ is a positive solution of $x^2 + a^2 = y^p$ such that $x \geq a^2, \gcd(x,y) = 1$ then*

$$(a,x,y,p) \in \{(7,524,65,3),(97,1405096,12545,3),(135,140374,2701,3)\}.$$

3.2. **Remark on the case of fixed p.** Let $I(N)$ denote the set of odd integers less than or equal to N. To resolve (1) completely for a fixed prime p and $a \in I(N)$ an obvious method is to find all integral solution of the polynomial equations

$$G_p(-\delta v + a_0, v) = a, \quad \text{for } a_0 | a \text{ and } a_0 \equiv a \bmod p.$$

We will refer to this method as method I. Method II will mean that we solve the polynomial equations (6) and determine all integral solutions of the Thue equation

$$\frac{G_p(X,Y)}{X + \delta Y} = 1.$$

Solving Thue equations of high degree is a difficult task, but in certain cases it is possible (see [10],[11],[12],[21]). In the following table in the first row we indicate the running times needed to resolve (1) for $p = 5, 7$ and 11, and for odd integers $a \in \{1, \ldots, 5001\}$ using method I. The second row contains the running times in case of method II. We note that in case of $p = 3$ method II does not apply, since the degree of the polynomial $\frac{G_p(X,Y)}{X+\delta Y}$ is 2.

$1 \leq a \leq 5001$	$p = 5$	$p = 7$	$p = 11$
method I.	7.26 sec	52 sec	310 sec
method II.	3.34 sec	8.34 sec	100 sec

The complete lists of solutions in these cases are given by:

- $p = 5$:

$$\begin{aligned}(a,x,y) \in \{&(3,79,5),(79,3,5),(475,719,13),(475,11767,37),(717,1525,17),\\ &(2807,5757,29),(2879,3353,25),(3353,2879,25)\},\end{aligned}$$

- $p = 7$:

$$(a,x,y) \in \{(249,307,5),(307,249,5),(2105,11003,13)\},$$

- $p = 11$:

$$(a,x,y) \in \{(3827,9111,5)\}.$$

Acknowledgment. I would like to thank my supervisor Robert Tijdeman, Lajos Hajdu, Yann Bugeaud and Jan-Hendrik Evertse for their valuable remarks and suggestions.

References

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

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

[3] S. A. Arif, F. S. A. Muriefah, *The Diophantine equation* $x^2 + 3^m = y^n$ Internat. J. Math. Math. Sci., **21** (1998), 619-620.
[4] S. A. Arif, F. S. A. Muriefah, *The Diophantine equation* $x^2 + 5^{2k+1} = y^n$, Indian J. Pure Appl. Math., **30** (1999), 229-231.
[5] S. A. Arif, F. S. A. Muriefah, *The Diophantine equation* $x^2 + q^{2k} = y^n$, Arab. J. Sci. Eng. Sect. A Sci., **26** (2001), 53-62.
[6] S. A. Arif, F. S. A. Muriefah, *On the Diophantine equation* $x^2 + q^{2k+1} = y^n$, J. Number Theory, **95** (2002), 95-100.
[7] S. A. Arif, F. S. A. Muriefah, *On the Diophantine equation* $x^2 + 2^k = y^n$ *II*, Arab J. Math. Sci., **7** (2001), 67-71.
[8] M. Bauer, M. A. Bennett, *Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation*, Ramanujan J., **6** (2002), 209-270.
[9] F. Beukers, *The Diophantine equation* $Ax^p + By^q = Cz^r$, Duke Math. J., **91** (1998), 61-88.
[10] Yu. Bilu, G. Hanrot, *Solving Thue equations of high degree*, J. Number Theory, **60** (1996), 373-392.
[11] Yu. Bilu, G. Hanrot, *Thue equations with composite fields*, Acta Arith., **88** (1999), 311-326.
[12] Yu. Bilu, G. Hanrot, P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math., **539** (2001), 75-122.
[13] Y. Bugeaud, *On the Diophantine equation* $x^2 - p^m = y^n$, Acta Arith. **80** (1997), 213-223.
[14] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, 138, Springer-Verlag, Berlin, 1993.
[15] J. H. E. Cohn, *The diophantine equation* $x^2 + 2^k = y^n$, Arch. Math. (Basel), **59** (1992), 341-344.
[16] J. H. E. Cohn, *The diophantine equation* $x^2 + C = y^n$, Acta Arith., **65** (1993), 367-381.
[17] J. H. E. Cohn, *Perfect Pell powers*, Glasgow Math. J., **38** (1996), 19-20.
[18] J. H. E. Cohn, *The Diophantine equation* $x^2 + 2^k = y^n$ *II*, Internat. J. Math. Math. Sci., **22** (1999), 459-462.
[19] J. H. E. Cohn, *The Diophantine equation* $x^2 + C = y^n$ *II*, Acta Arith., **109** (2003), 205-206.
[20] H. Darmon, A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc, **27** (1995), 513-543.
[21] G. Hanrot, *Solving Thue equations without the full unit group*, Math. Comp., **69** (2000), 395-405.
[22] C. Ko, *On the diophantine equation* $x^2 = y^n + 1, xy \neq 0$, Sci. Sinica, **14** (1965), 457-460.
[23] W. Ljunggren, *Über die Gleichungen* $1 + Dx^2 = 2y^n$ *und* $1 + Dx^2 = 4y^n$, Norske Vid. Selsk. Forh., Trondhjem, **15** (1942), 115-118.
[24] W. Ljunggren, *On the Diophantine equation* $x^2 + p^2 = y^n$, Norske Vid. Selsk. Forh., Trondhjem **16** (1943), 27-30.
[25] W. Ljunggren, *On the diophantine equation* $Cx^2 + D = y^n$, Pacific. J. Math., **14** (1964), 585-596.
[26] W. Ljunggren, *On the diophantine equation* $Cx^2 + D = 2y^n$, Math. Scand., **18** (1966), 69-86.
[27] F. Luca, *On a diophantine equation*, Bull. Austral. Math. Soc., **61** (2000), 241-246.
[28] F. Luca, *On the equation* $x^2 + 2^a 3^b = y^n$, Internat. J. Math. Math. Sci., **29** (2002), 239-244.
[29] M. Mignotte, *On the Diophantine equation* $D_1 x^2 + D_2^m = 4y^n$, Portugal. Math. **54** (1997), 457-460.

[30] M. Mignotte, *A corollary to a theorem of Laurent-Mignotte-Nesterenko*, Acta Arith., **86** (1998), 101-111.
[31] L. J. Mordell, *Diophantine equations*, Pure and Applied Mathematics, Vol. 30, Academic Press, London, 1969.
[32] F. S. A. Muriefah, *On the Diophantine equation* $Ax^2 + 2^{2m} = y^n$, Internat. J. Math. Math. Sci., **25** (2001), 373-381.
[33] F. S. A. Muriefah, *On the Diophantine equation* $px^2 + 3^n = y^p$, Tamkang J. Math., **31** (2000), 79-84.
[34] T. Nagell, *Verallgemeinerung eines Fermatschen Satzes*, Arch. Math. (Basel), **5** (1954), 153-159.
[35] I. Niven, *Irrational numbers*, The Carus Mathematical Monographs, No. 11. Distributed by John Wiley and Sons, Inc., New York, 1956.
[36] I. Pink, Sz. Tengely, *Full powers in arithmetic progressions*, Publ. Math. Debrecen, **57** (2000), 535-545.
[37] I. Pink, *On the Diophantine equation* $x^2 + (p_1^{z_1} \cdots p_s^{z_s})^2 = 2y^n$, to appear.
[38] A. Schinzel, R. Tijdeman, *On the equation* $y^m = P(x)$, Acta Arith. **31** (1976), 199-204.
[39] S. Siksek, J. E. Cremona, *On the Diophantine Equation* $x^2 + 7 = y^m$, Acta Arith., **109** (2003), 143-149.
[40] B. Sury, *On the Diophantine equation* $x^2 + 2 = y^n$, Arch. Math. (Basel), **74** (2000), 350-355.

Mathematical Institute
Leiden University
P.O.Box 9512
2300 RA Leiden
The Netherlands
E-mail address: tengely@math.leidenuniv.nl