

RESEARCH

Open Access



# An upper bound for solutions of the Lebesgue-Nagell equation $x^2 + a^2 = y^n$

Xiaowei Pan\*

\*Correspondence:  
panda1211@163.com  
Xi'an Medical University, Xi'an,  
Shaanxi, P.R. China

## Abstract

Let  $a$  be a positive integer with  $a > 1$ , and let  $(x, y, n)$  be a positive integer solution of the equation  $x^2 + a^2 = y^n$ ,  $\gcd(x, y) = 1$ ,  $n > 2$ . Using Baker's method, we prove that, for any positive number  $\epsilon$ , if  $n$  is an odd integer with  $n > C(\epsilon)$ , where  $C(\epsilon)$  is an effectively computable constant depending only on  $\epsilon$ , then  $n < (2 + \epsilon)(\log a)/\log y$ . Owing to the obvious fact that every solution  $(x, y, n)$  of the equation satisfies  $n > 2(\log a)/\log y$ , the above upper bound is optimal.

**MSC:** 11D61

**Keywords:** exponential diophantine equation; Lebesgue-Nagell equation; upper bound for solutions; Baker's method

## 1 Introduction

Let  $\mathbb{Z}$ ,  $\mathbb{N}$  be the sets of all integers and positive integers, respectively. Let  $D$  be a positive integer. In 1850, Lebesgue [1] proved that if  $D = 1$ , then the equation

$$x^2 + D = y^n, \quad x, y, n \in \mathbb{N}, \gcd(x, y) = 1, n > 2 \quad (1.1)$$

has no solutions  $(x, y, n)$ , which solved a type important case of the famous Catalan's conjecture. From then on, Nagell [2–4] dealt with the solution of (1.1) more systematically for the case of  $D > 1$ . Therefore, equation (1.1) is called the Lebesgue-Nagell equation (see [5]).

In this paper, we shall discuss an upper bound for solutions of (1.1) when  $D > 1$ , that is,  $D = a^2$ , where  $a$  is a positive integer with  $a > 1$ . So equation (1.1) can be expressed as

$$x^2 + a^2 = y^n, \quad x, y, n \in \mathbb{N}, \gcd(x, y) = 1, n > 2. \quad (1.2)$$

This is a type of Lebesgue-Nagell equation leading to more discussions (see [6]). Let  $(x, y, n)$  be a solution of (1.2). In 2004, Tengely [7] proved that if  $y > 50,000$  and  $n$  is an odd prime with  $n > 9,511$ , then

$$n < \frac{4 \log a}{\log 50,000}. \quad (1.3)$$

Using Baker's method, the following result is proved.

**Theorem** For any positive number  $\epsilon$ , if  $n$  is an odd number with  $n > C(\epsilon)$ , then

$$n < \frac{(2 + \epsilon) \log a}{\log y}, \quad (1.4)$$

where  $C(\epsilon)$  is an effectively computable constant depending only on  $\epsilon$ .

Owing to (1.2) every solution  $(x, y, n)$  of the equation satisfies  $a^2 < y^n$ , then we have

$$n > \frac{2(\log a)}{\log y}. \quad (1.5)$$

Hence comparing (1.4) and (1.5), we see that the upper bound we get in this paper is optimal.

## 2 Preliminaries

**Lemma 2.1** For a positive odd integer  $n$ , every solution  $(X, Y, Z)$  of the equation

$$X^2 + Y^2 = Z^n, \quad X, Y, Z \in \mathbb{N}, \gcd(X, Y) = 1 \quad (2.1)$$

can be expressed as

$$\begin{aligned} Z &= f^2 + g^2, \quad X + Y\sqrt{-1} = \lambda_1(f + \lambda_2 g\sqrt{-1})^n, \quad f, g \in \mathbb{N}, \\ \gcd(f, g) &= 1, \quad \lambda_1, \lambda_2 \in \{1, -1\}. \end{aligned} \quad (2.2)$$

*Proof* See Section 15.2 of [8].  $\square$

Let  $\alpha$  be an algebraic number of degree  $d$ ,  $c$  be a leading coefficient of the defined polynomial of  $\alpha$ ,  $\alpha^{(j)}$  ( $j = 1, \dots, d$ ) be the whole conjugate numbers of  $\alpha$ . Then

$$h(\alpha) = \frac{1}{d} \left( \log c + \sum_{j=1}^d \log \max\{1, |\alpha^{(j)}|\} \right) \quad (2.3)$$

is called the Weil height of  $\alpha$ .

**Lemma 2.2** For the positive integers  $b_1$  and  $b_2$ , assume

$$\Lambda = b_1 \log \alpha - b_2 \pi \sqrt{-1}, \quad (2.4)$$

where  $\log \alpha$  is principal value of the logarithm of  $\alpha$ . If  $|\alpha| = 1$  and  $\alpha$  is not a unit root, then

$$\log |\Lambda| \geq -8.87AB^2, \quad (2.5)$$

where

$$\begin{aligned} A &= \max \left\{ 20, 10.98 |\log \alpha| + \frac{1}{2} dh(\alpha) \right\}, \\ B &= \max \left\{ 17, \frac{\sqrt{d}}{40}, 5.03 + 2.35 \left( \frac{d}{2} \right) + \frac{d}{2} \left( \frac{b_1}{68.9} + \frac{b_2}{2A} \right) \right\}. \end{aligned}$$

*Proof* See Theorem 3 of [9]. □

### 3 Proof of theorem

Let  $(x, y, n)$  be a solution of equation (1.2) with  $n$  being odd and satisfying

$$n > \frac{(2 + \epsilon) \log a}{\log y}. \quad (3.1)$$

By (1.2), we see that equation (2.1) has the solution  $(X, Y, Z) = (x, a, y)$ . So from Lemma 2.1, we get

$$y = f^2 + g^2, \quad f, g \in \mathbb{N}, \gcd(f, g) = 1, \quad (3.2)$$

$$x + a\sqrt{-1} = \lambda_1(f + \lambda_2 g\sqrt{-1})^n, \quad \lambda_1, \lambda_2 \in \{1, -1\}. \quad (3.3)$$

Assume

$$\theta = f + g\sqrt{-1}, \quad \bar{\theta} = f - g\sqrt{-1}. \quad (3.4)$$

From (3.2) and (3.4), we have

$$\theta \bar{\theta} = y, \quad |\theta| = |\bar{\theta}| = \sqrt{y}. \quad (3.5)$$

Let  $\alpha = \theta/\bar{\theta}$ . From (3.4) and (3.5), we see that  $\alpha$  satisfies  $|\alpha| = 1$  and

$$y\alpha^2 - 2(f^2 - g^2)\alpha + y = 0. \quad (3.6)$$

Since  $\gcd(x, y) = 1$  by (1.1) and  $n > 2$ , we have  $\gcd(x, a) = 1$  and  $y$  is odd. And since  $\gcd(f, g) = 1$  from (3.2), we see  $f$  is odd,  $g$  is even, so  $\gcd(f^2 + g^2, f^2 - g^2) = \gcd(f^2 + g^2, 2(f^2 - g^2)) = 1$ . Hence  $y > 1$  and we see that  $\alpha$  is not a unit root. And since the discriminant of the polynomial  $yz^2 - 2(f^2 - g^2)z + y \in \mathbb{Z}[z]$  is equal to  $-16f^2g^2$ , we see that  $\alpha$  is a quadratic algebraic number,  $\alpha$  and  $\alpha^{-1}$  are its whole conjugate numbers. Thus by (2.3), we deduce that the Weil height of  $\alpha$  is

$$h(\alpha) = \frac{1}{2} \log y. \quad (3.7)$$

Since by (3.3) we have

$$x - a\sqrt{-1} = \lambda_1(f - \lambda_2 g\sqrt{-1})^n, \quad (3.8)$$

from (3.3), (3.4), (3.5), and (3.8), we obtain

$$a = \left| \frac{\theta^n - \bar{\theta}^n}{2\sqrt{-1}} \right| = \frac{1}{2} |\theta^n - \bar{\theta}^n| = \frac{1}{2} |\bar{\theta}^n| \left| \left( \frac{\theta}{\bar{\theta}} \right)^n - 1 \right| = \frac{y^{n/2}}{2} |\alpha^n - 1|. \quad (3.9)$$

According to the maximum modulus principle, for any complex number  $z$ , we are sure that

$$|e^z - 1| \geq \frac{1}{2} \quad (3.10)$$

or

$$|e^z - 1| \geq \frac{2}{\pi} |z - k\pi\sqrt{-1}|, \quad k \in \mathbb{Z}. \quad (3.11)$$

Assume  $\alpha = e^z$ . If (3.10) holds, then from (3.9), we can deduce that

$$a \geq \frac{y^{n/2}}{4}. \quad (3.12)$$

Combining (3.1) and (3.12), we get

$$4 > y^{\epsilon n/2(2+\epsilon)}. \quad (3.13)$$

However, since  $y \geq 5$  by (3.2), we see that (3.13) does not hold when  $n > 2(2 + \epsilon)/\epsilon$ . Hence, we only need to discuss the case when (3.11) holds.

Owing to  $a^{2+\epsilon} < y^n$  by (3.1), if (3.11) holds, then from (3.9) and (3.11) we have

$$y^{n/(2+\epsilon)} > a \geq \frac{y^{n/2}}{\pi} |n \log \alpha - k\pi\sqrt{-1}|, \quad k \in \mathbb{N}, k \leq n. \quad (3.14)$$

Let

$$\Lambda = n \log \alpha - k\pi\sqrt{-1}. \quad (3.15)$$

By (3.14) and (3.15), we see

$$\log \pi - \log |\Lambda| \geq \frac{\epsilon n}{2(2 + \epsilon)} \log y. \quad (3.16)$$

Since we have proved that  $\alpha$  is not only a quadratic algebraic number but also a non-unit root with  $|\alpha| = 1$ , and the degree of  $\alpha$  is 2, from Lemma 2.2, by (3.7), we see that  $\Lambda$  satisfies (2.5), where

$$A = \max \left\{ 20, 10.98 |\log \alpha| + \frac{1}{2} \log y \right\}, \quad (3.17)$$

$$B = \max \left\{ 17, 7.38 + \log \left( \frac{n}{2A} + \frac{k}{68.9} \right) \right\}. \quad (3.18)$$

Since  $y \geq 5$  and the principal value of the logarithm of  $\alpha$  satisfies  $|\log \alpha| \leq \pi$ , we deduce by (3.17) that

$$A \leq 10.98\pi + \frac{1}{2} \log y. \quad (3.19)$$

By (3.14) and (3.17), we have  $k \leq n$  and  $1/(2A) \leq 0.025$ , respectively, therefore if  $n > 68.9 \times 10^8$ , then by (3.18) we get

$$B < 7.38 + \log(0.04n) < 4.17 + \log n. \quad (3.20)$$

Hence from (2.5), (3.16), (3.19), and (3.20), we have

$$\log \pi + 8.87 \left( 10.98\pi + \frac{1}{2} \log y \right) (4.17 + \log n)^2 > \frac{\epsilon n}{2(2 + \epsilon)} \log y. \quad (3.21)$$

Since  $y \geq 5$ , we see by (3.21) that

$$\frac{2(2 + \epsilon)}{\epsilon} (1 + 194.56(4.17 + \log n)^2) > n. \quad (3.22)$$

From (3.22), we get  $n < C'(\epsilon)$ , where  $C'(\epsilon)$  is an effectively computable constant depending only on  $\epsilon$ . Let

$$C(\epsilon) = \max \left\{ 68.9 \times 10^8, \frac{2(2 + \epsilon)}{\epsilon}, C'(\epsilon) \right\}. \quad (3.23)$$

We see by (3.23) that  $C(\epsilon)$  is also an effectively computable constant depending only on  $\epsilon$ , and to sum up, we can deduce when  $n > C(\epsilon)$ , the solution  $(x, y, n)$  of equation (1.2) does not satisfy (3.1), so (1.4) holds definitely. Therefore, we completed the proof of the theorem.

#### Competing interests

The author declares that they have no competing interests.

#### Acknowledgements

This work is supported by the National Natural Science Foundation of China (No. 11526162) and the Natural Science Foundation of Shaanxi Province (No. 2016JQ1040).

Received: 15 July 2016 Accepted: 26 August 2016 Published online: 02 September 2016

#### References

1. Lebesgue, VA: Sur l'impossibilité en nombres entiers de l'équation  $x^m = y^2 + 1$ . *Nouv. Ann. Math.* **9**(2), 178-181 (1850)
2. Nagell, T: Sur l'impossibilité de quelques équations à deux indéterminées. *Norsk. Mat. Forenings Skrifter* **13**(1), 65-82 (1921)
3. Nagell, T: Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante. *Math. Z.* **28**(1), 10-29 (1928)
4. Nagell, T: Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns. *Nova Acta R. Soc. Sci. Ups.* **16**(2), 1-38 (1955)
5. Bugeaud, Y, Mignotte, M, Siksek, S: Classical and modular approaches to exponential Diophantine equations II: the Lebesgue-Nagell equation. *Compos. Math.* **142**(1), 31-62 (2006)
6. Le, MH, Hu, YZ: New Advances on the generalized Lebesgue-Ramanujan-Nagell equation. *Adv. Math.* **41**(4), 385-396 (2012)
7. Tengely, S: On the Diophantine equation  $x^2 + a^2 = 2y^p$ . *Indag. Math.* **15**(2), 291-304 (2004)
8. Mordell, LJ: *Diophantine Equations*. Academic Press, London (1969)
9. Laurent, M, Mignotte, M, Nesterenko, Y: Formes linéaires en deux logarithmes et déterminants d'interpolation. *J. Number Theory* **55**(2), 285-321 (1995)