Revista Colombiana de Matemáticas
Volumen 40 (2006), páginas 31–37

The Diophantine equation $x^2 + c = y^n$: a brief overview

Fadwa S. Abu Muriefah
Girls College Of Education, Saudi Arabia

Yann Bugeaud
Université Louis Pasteur, France

Abstract. We give a survey on recent results on the Diophantine equation $x^2 + c = y^n$.

Key words and phrases. Diophantine equations, Baker's method.

2000 Mathematics Subject Classification. Primary: 11D61.

Resumen. Nosotros hacemos una revisión acerca de resultados recientes sobre la ecuación Diofántica $x^2 + c = y^n$.

1. Who was Diophantus?

The expression 'Diophantine equation' comes from Diophantus of Alexandria (about A.D. 250), one of the greatest mathematicians of the Greek civilization. He was the first writer who initiated a systematic study of the solutions of equations in integers. He wrote three works, the most important of them being 'Arithmetic', which is related to the theory of numbers as distinct from computation, and covers much that is now included in Algebra. Diophantus introduced a better algebraic symbolism than had been known before his time. Also in this book we find the first systematic use of mathematical notation, although the signs employed are of the nature of abbreviations for words rather than algebraic symbols in contemporary mathematics. Special symbols are introduced to present frequently occurring concepts such as the unknown up

to its sixth power. He stands out in the history of science as one of the great unexplained geniuses. A Diophantine equation or indeterminate equation is one which is to be solved in integral values of the unknowns.

The fundamental problem when studying a given Diophantine equation is whether a solution exists, and, in the case it exists, how many solutions there are. A very important problem closely related to the previous one is the question of the actual computation of the existing solutions or whether there is a general form for the solutions. For more information, we refer the reader to the books [32, 36].

2. The Diophantine equation $f(x) = y^n$

Let $f(X)$ be an irreducible polynomial with integer coefficients and of degree $m \geq 2$. Let $n \geq 2$ be an integer. Since the work of Siegel, we know that the Diophantine equation

$$f(x) = y^n, \quad \text{in integers } x,\, y, \tag{1}$$

has only finitely many solutions, provided that $(m, n) \neq (2, 2)$. Several papers deal with (1) or particular cases from (1). In particular, there is a very broad literature on the Diophantine equations

$$ax^2 + bx + c = dy^n, \quad \text{in integers } x,\, y,\, n \geq 3, \tag{2}$$

and

$$ax^2 + bx + c = dy^n, \quad \text{in integers } x,\, n \geq 3, \tag{3}$$

where a, b, c and d are fixed integers, and y is a fixed integer in (3).

3. The Diophantine equation $x^2 + c = y^n$

In the present survey, we restrict our attention to the Diophantine equation

$$x^2 + c = y^n, \quad \text{in integers } x,\, y,\, n \geq 3, \tag{4}$$

where c is a *positive* integer.

The first result on (4) seems to be the proof in 1850 by V. A. Lebesgue [20] that there are no non-trivial solutions for $c = 1$. He assumed that there exist positive integers x, y and $n \geq 3$ such that $x^2 + 1 = y^n$. He then worked in the ring of Gaussian integers, estimated the 2-adic valuation of various quantities and reached eventually a contradiction.

The next cases to be solved were $c = 3$ and $c = 5$ by Nagell [27] (see also [28]) in 1923. It is for this reason that equation (4) is called the Lebesgue–Nagell equation in [12]. Then, Ljunggren [22] established that equation (4) with $c = 2$ has only the solution $5^2 + 2 = 3^3$. The case $D = 4$ was subsequently solved by Nagell [30]: the only solutions are $2^2 + 4 = 2^3$ and $11^2 + 4 = 5^3$. As pointed

out by Cohn [14], there are numerous cases of duplication of known results: for instance, Ljunggren's result on the case $c = 2$ has been later rediscovered by Nagell [29] (note that, recently, a more elementary proof has been given by Sury [37]). Note that Nagell's works have been collected by Ribenboim [31].

The next important step is an article by Cohn [14], where he completed the solutions for 77 values of c in the range $1 \leq c \leq 100$. His methods are ingenious and elementary, in the sense that they do not rest on deep tools from Diophantine approximation. His paper also contains an extensive list of references on earlier works on (4).

The smallest value of c not treated by Cohn is $c = 7$. The difficulty comes from the fact that $2 = (1 + \sqrt{-7})(1 - \sqrt{-7})$ in the field $\mathbf{Q}(\sqrt{-7})$, as will be explained in the next section.

The solutions for the cases $c = 74$, 86 were completed by Mignotte and de Weger [26] (indeed, Cohn solved these two equations of type (4) except for $p = 5$, in which case difficulties occur since the class numbers of the corresponding imaginary quadratic fields are divisible by 5). Bennett and Skinner (Proposition 8.5 of [9]) applied the modular approach to solve the cases $D = 55$ and 95. The 19 remaining values, namely

$$c = 7,\ 15,\ 18,\ 23,\ 25,\ 28,\ 31,\ 39,\ 45,\ 47,\ 60,\ 63,\ 71,\ 72,\ 79,\ 87,\ 92,\ 99,\ 100, \tag{5}$$

are clearly beyond the scope of Cohn's elementary method, and were solved in 2004 by Bugeaud, Mignotte and Siksek [12].

4. Methods and difficulties

The starting point when dealing with equation (4) is to factor it over the quadratic field $\mathbf{K}$ generated by $\sqrt{-c}$. In the sequel, we assume that n is an odd prime, and we choose to denote it by p. Assume that (x, y, p) is a solution of (4) and write

$$(x + \sqrt{-c}) \cdot (x - \sqrt{-c}) = y^p.$$

We would like to conclude that both $x + \sqrt{-c}$ and $x + \sqrt{-c}$ are then perfect p-th powers in $\mathbf{K}$. Unfortunately, this is far from being always the case.

A first problem occurs when $x + \sqrt{-c}$ and $x + \sqrt{-c}$ are not coprime. We can then only conclude that both numbers are 'almost' perfect p-th powers. Observe that the greatest common divisor in the ring of algebraic integers of $\mathbf{K}$ of $x + \sqrt{-c}$ and $x + \sqrt{-c}$ divides both $2x$ and $2\sqrt{-c}$. Furthermore, if c is squarefree, then x and $\sqrt{-c}$ are necessarily coprime, and a problem may only occur when 2 splits in the number field $\mathbf{K}$, that is, when c is congruent to 7 modulo 8. If c is not squarefree, then (4) may have a solution (x, y, p) with $\gcd(x, y) > 1$.

A second problem occurs when p divides the class number of the quadratic field $\mathbf{K}$. Then, the principal ideal π generated by $x + \sqrt{-c}$ can be written

under the form $\pi = \xi^p$, for some ideal ξ, but it is not always the case that ξ is principal.

A third problem occurs when $\mathbf{K} = \mathbf{Q}(\sqrt{-1})$ or $\mathbf{Q}(\sqrt{-3})$, that is, when there exist in $\mathbf{K}$ units other than ± 1 (see [14], Lemma 2).

The main methods used in [12] for attacking equation (4) are linear forms in logarithms (to bound p) and the modular approach, though for some small values of p it is necessary to reduce the equation to a family of Thue equations. The tools for reducing equation (4) to Thue equations are well-known.

For all the 19 remaining examples, estimates for linear forms in *three* variables (and not in *two*: Le's paper [17] is erroneous) are needed. The current best bounds are due to Mignotte [25] and lead to upper estimates for p (in our range of values for c) being comprised between 10^8 and 2.4×10^9. Then, the authors of [12] used the modular method, which is very well explained by Siksek in the expository paper [34] (see also [35]), to solve equation (4) for all values of c listed at (5). A sample of their result is the following.

Theorem ([12]). *The Diophantine equation $x^2 + 7 = y^n$ in positive integers x, y and $n \geq 3$, has only the solutions given by*

$$(x, y, n) \in \{(1, 2, 3), (3, 2, 4), (5, 2, 5), (11, 2, 7), (181, 2, 15)\}.$$

The above Theorem shows that the equation $x^2 + 7 = y^n$ has no more solutions than the equation $x^2 + 7 = 2^n$. Earlier results on $x^2 + 7 = y^n$ are due to Lesage [21] and to Siksek and Cremona [35].

5. The BHV Theorem

Yu. Bilu, G. Hanrot and P. M. Voutier [11] completely solved the problem of existence of primitive divisors in Lucas–Lehmer sequences. Their deep result, which we refer to as the 'Theorem BHV', turns out to have many applications to Diophantine equations, and, in particular, to equation (4). Indeed, as observed by Cohn [16], the equations solved in his paper [14] can now easily be solved by using Theorem BHV.

This theorem has also been applied in several papers [23, 7, 24] whose results are discussed in the next section. Furthermore, it has been used in many works on equations of type (1), see for instance [10].

6. The Diophantine equation $x^2 + c = y^n$, with c in some infinite set

Several authors have studied various extensions of equation (4). Cohn [13] showed that if $c = 2^{2k+1}$, then equation (4) has solutions only when $n = 3$ and in this case there are three families of solutions. He also pointed out that the case $c = 2^{2k}$ is much more difficult. Arif and Abu Muriefah [5] conjectured that the only solutions are then given by $(x, y) = \left(2^k, 2^{2k+1}\right)$ and

$(x, y) = \left(11 \cdot 2^{k-1}, 5 \cdot 2^{2(k-1)/3}\right)$, with the latter solution existing only when $(k, n) = (3M + 1, 3)$ for some integer $M \geq 0$. Partial results towards this conjecture were obtained in [5, 15], and it was finally proved by Arif and Abu Muriefah [7]. Alternative proofs are due to Le [18] and to Siksek [33].

Luca [23] was able to prove the conjecture of Abu Muriefah and Arif [2] concerning the solutions of the Diophantine equation $x^2+3^{2m} = y^n$. Subsequently, Luca [24] solved completely the case $c = 2^a 3^b$, under the additional assumption that x and y are coprime. Here, a and b denote arbitrary non-negative integers.

Arif and Abu Muriefah [6] proved that if $c = 3^{2k+1}$, then (4) has exactly one (infinite) family of solutions. The case $c = 3^{2k}$ has been solved by Luca [23] under the additional hypothesis that x and y are coprime.

Abu Muriefah [1] established that if $c = 5^{2k}$, then equation (4) may have a solution only if 5 divides x and p does not divide k for any odd prime p dividing n. Abu Muriefah and Arif [3] proved that if $c = 5^{2k+1}$, then (4) has no solutions for all $k \geq 0$. They further obtained several results [4] if $c = q^{2k}$, where q is an odd prime.

Let $q \geq 11$ be an odd prime number not congruent to 7 modulo 8. Arif and Abu Muriefah [8] established that (4) with $c = q^{2k+1}$, $n \geq 5$ odd and coprime with the class number of $\mathbf{Q}(\sqrt{-q})$, has exactly two families of solutions.

In the very particular case when c is the square of an odd prime number, Le [19] gave rather complicated, but very strong necessary conditions for the solutions (x, y, n) of (4) satisfying the additional assumption $\gcd(x, y) = 1$.

Acknowledgements We are pleased to thank the referee for his very careful reading of a first version of our text.

References

[1] F. S. Abu Muriefah, *On the Diophantine equation* $x^2 + 5^{2k} = y^n$, Demo. Math. (To appear).

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

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

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

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

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

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

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

[9] M. A. Bennett & C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56 [1]** (2004), 23–54.

[10] Yu. Bilu, *On Le's & Bugeaud's papers about the equation* $ax^2+b^{2m-1} = 4c^p$, Monatsh. Math. **137** (2002), 1–3.

[11] Yu. Bilu, G. Hanrot, & P. M. Voutier, with an appendix by M. Mignotte, *Existence of primitive divisors of Lucas and Lehmer sequences*, J. Reine Angew. Math. **539** (2001), 75–122.

[12] Y. Bugeaud, M. Mignotte & S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell equation*, Compositio Math. **142** (2006), 31–62.

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

[14] J. H. E. Cohn, *The Diophantine equation* $x^2+C = y^n$, Acta Arith. **65** (1993), 367–381.

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

[16] J. H. E. Cohn, *The Diophantine equation* $x^2 + C = y^n$. *II*, Acta Arith. **109** (2003), 205–206.

[17] Maohua Le, *A note on the Diophantine equation* $x^2 + 7 = y^n$, Glasgow Math. J. **39** (1997), 59–63.

[18] M. Le, *On Cohn's conjecture concerning the Diophantine equation* $x^2+2^m = y^n$, Arch. Math. (Basel) **78** [**1**] (2002), 26–35.

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

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

[21] J.-L. Lesage, *Différence entre puissances et carrés d'entiers*, J. Number Theory **73** (1998), 390–425.

[22] W. Ljunggren, *Über einige Arcustangensgleichungen die auf interessante unbestimmte Gleichungen führen*, Ark. Mat. Astr. Fys. **29A** [**13**] (1943).

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

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

[25] M. Mignotte, *A kit on linear forms in three logarithms*, IRMA, Strasbourg, to appear.

[26] M. Mignotte & B. M. M. de Weger, *On the Diophantine equations* $x^2 + 74 = y^5$ *and* $x^2 + 86 = y^5$, Glasgow Math. J. **38** (1996), 77–85.

[27] T. Nagell, *Sur l'impossibilité de quelques équations à deux indéterminées*, Norsk Mat. Forensings Skrifter **13** (1923), 65–82.

[28] T. Nagell, *Lφsning til oppgave nr 2, 1943, s. 29*, Nordisk Mat. Tidskr. **30** (1948), 62–64.

[29] T. Nagell, *Verallgemeinerung eines Fermatschen Satzes*, Arch. Math. (Basel) **5** (1954), 153–159.

[30] T. Nagell, *Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns*, Nova Acta Regiae Soc. Sci. Upsaliensis 4 **16** [**2**] (1955).

[31] T. Nagell, *Collected papers of Trygve Nagell. Vol. 1–4.*, Edited by Paulo Ribenboim. Queen's Papers in Pure and Applied Mathematics, Queen's University 121, Kingston, ON, 2002.

[32] T. N. Shorey & R. Tijdeman, *Exponential Diophantine equations*, Cambridge University Press, Cambridge, 1986.

[33] S. Siksek, *On the Diophantine equation* $x^2 = y^p + 2^k z^p$, J. Théor. Nombres Bordeaux **15** (2003), 839–846.

[34] S. Siksek, *The modular approach to Diophantine equations.*, In: Explicit Methods in Number Theory, Panoramas et Synthèses,, Société Mathématique De France, to appear.

[35] S. Siksek & J. E. Cremona, *On the Diophantine equation* $x^2 + 7 = y^m$, Acta Arith. **109** (2003), 143–149.

[36] V. G. Sprindžuk, *Classical Diophantine equations*, Lecture Notes in Mathematics 1559, Springer–Verlag, Berlin, 1993.

[37] B. Sury, *On the Diophantine equation* $x^2 + 2 = y^n$, Arch. Math. (Basel) **74** (2000), 350–355.

(Recibido en octubre de 2005. Aceptado en febrero de 2006)

Mathematics Department
Girls College Of Education
P.O. Box 60561
Riyadh 11555, Saudi Arabia
e-mail: abumuriefah@yahoo.com

U. F. R. de mathématiques
Université Louis Pasteur
7, rue René Descartes
67084 Strasbourg Cedex, France
e-mail: bugeaud@math.u-strasbg.fr