Publ. Math. Debrecen
64/1-2 (2004), 21–30

A note on the Ramanujan–Nagell equation

By E. HERRMANN (Saarbrücken), F. LUCA (Morelia)
and P. G. WALSH (Ottawa)

Abstract. In the present paper we determine all positive integer solutions to the equation $x^2+7y^4=k$, where k is a positive integer divisible only by primes less than 12.

1. Introduction

It is an amusing fact, noticed by Ramanujan, that the sequence 2^n-7 takes on square values for $n=3,4,5,7$ and again for $n=15$. In 1960, NAGELL [13] published a proof that the only solutions in positive integers (n,x) to the equation

$$x^2+7=2^n \tag{1.1}$$

are $(n,x)=(3,1),(4,3),(5,5),(7,11),(15,181)$, thereby completely solving the problem posed by Ramanujan. Since then, a vast literature on these types of diophantine problems has been generated. Numerous different proofs of Nagell's theorem have appeared, such as Hasse's simple proof which is presented in MORDELL's book [12]. Many generalizations of the original problem have been posed and solved, such as the work by BEUKERS [2], [3] on the equation $x^2+D=p^n$, and recent improvements by BAUER and BENNETT [1]. A more general form of this problem is a diophantine

Mathematics Subject Classification: 11D25, 11B39.
Key words and phrases: cubic and quartic equations, Fibonacci and Lucas numbers and polynomials and generalizations.

equation of the type

$$f(x) = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r},$$

where $f(x)$ is a polynomial with integer coefficients and at least two simple zeros, $p_1, p_2, \ldots, p_r$ are rational primes, and $n_1, n_2, \ldots, n_r$ are non-negative integers. For a survey of the history of this topic, we refer the reader to the paper of Cohen [5], and to the above mentioned paper of Bauer and Bennett.

On a different matter, there have been many papers written on the topic of determining squares in linear recurrence sequences. In particular, Ljunggren (for example see [6]–[10]) proved many results on the solvability of diophantine equations of the form

$$ax^4 - by^2 = c, \tag{1.2}$$

with $c \in \{\pm 1, \pm 4\}$. For a survey of Ljunggren's work, and more recent developments, we refer the reader to [19].

Let (n, x) be a solution to equation (1.1). Using the fact that the ring of integers of the field $\mathbb{Q}(\sqrt{-7}\,)$ is a unique factorization domain, with no nontrivial units, it follows that

$$\frac{x \pm \sqrt{-7}}{2} = \pm \left(\frac{1 + \sqrt{-7}}{2} \right)^{n-2}.$$

For $n \geq 0$, define sequences $\{T_n\}$ and $\{U_n\}$ by the relation

$$\frac{T_n + U_n\sqrt{-7}}{2} = \left(\frac{1 + \sqrt{-7}}{2} \right)^{n}.$$

Nagell's theorem is the determination of those values of n for which $|U_n|=1$. It is natural to ask if there are any squares in the sequence $\{|U_n|\}$. In other words, determine the integer solutions (n, x, y) to the diophantine equation

$$x^2 + 7y^4 = 2^n. \tag{1.3}$$

This generalization of the Ramanujan–Nagell equation (equation (1.1)) has not been considered, at least to the knowledge of the present authors. Moreover, this type of problem is a natural complex analogue to those problems considered by Ljunggren in equation (1.2).

In [14], the authors use methods from Diophantine approximation and lattice basis reduction to generalize Nagell's theorem. In particular, they determine all integer solutions (x,k) to the more general equation $x^2+7=k$, where x is an integer, and k is an integer divisible only by primes less than 20. In consideration of this, and (1.3), the purpose of the present paper is to determine all positive integer solutions to the equation

$$x^2 + 7y^4 = k, \tag{1.4}$$

where k is a positive integer divisible only by primes less than 12. With more computation, one can increase the bound of 12.

Remark 1. Already from the result of K. Mahler [11] it follows that (1.3) and (1.4) have only finitely many solutions in rational integers. Later, S. V. Kotov [16] proved an effective version of Mahler's result. But neither (1.3) nor (1.4) were solved completely so far.

Definition 1. If (x,y,k) and (X,Y,K) are solutions to (1.4), we say that (X,Y,K) is a *multiple* of the solution (x,y,k) if either

i. $(X,Y,K)=(d^2x,dy,d^4k)$ for some positive integer d divisible only by primes less than 12, or

ii. $(X,Y,K)=(7d^2y^2m,dmu,7d^4m^2k)$, where $x=mu^2$ for integers m,u with m squarefree, and both d and m divisible only by primes less than 12.

2. A solution (x,y,k) to (1.4) is *minimal* if

i. whenever a prime p divides $\gcd(x,k)$, then p^4 does not divides k, and

ii. whenever 7 divides $\gcd(x,k)$, then the numerator of the reduced form of $x/(7y)$ is not the square of an integer.

If a solution (x,y,k) of (1.4) fails to satisfy condition (i), then it is easy to see that it is a multiple of a smaller solution. If (x,y,k) satisfies condition (i) but fails to satisfy condition (ii), then it is a multiple of the smaller solution $(7y^2/g,\sqrt{x/g},7k/g^2)$, where $g=\gcd(x,7y)$. Therefore, we will restrict our attention to the problem of determining all minimal solutions to equation (1.4).

x	y	k	x	y	k
1	1	2^3	147	3	$2^5 \cdot 3^2 \cdot 7 \cdot 11$
2	1	11	170	5	$5^2 \cdot 11^3$
3	1	2^4	181	1	2^{15}
3	2	11^2	205	3	$2^5 \cdot 11^3$
3	3	$2^6 \cdot 3^2$	235	15	$2^{14} \cdot 5^2$
5	1	2^5	273	1	$2^3 \cdot 7 \cdot 11^3$
5	5	$2^4 \cdot 5^2 \cdot 11$	285	15	$2^4 \cdot 3^3 \cdot 5^3 \cdot 11^2$
9	1	$2^4 \cdot 11$	435	5	$2^6 \cdot 5^2 \cdot 11^2$
11	1	2^7	525	53	$2^{16} \cdot 7 \cdot 11^2$
13	1	$2^4 \cdot 11$	595	5	$2^{11} \cdot 5^2 \cdot 7$
15	3	$2^3 \cdot 3^2 \cdot 7$	618	12	$2^2 \cdot 3^2 \cdot 11^4$
21	1	$2^6 \cdot 7$	627	11	$2^{12} \cdot 11^2$
29	3	$2^7 \cdot 11$	931	3	$2^{10} \cdot 7 \cdot 11^2$
31	1	$2^3 \cdot 11^2$	987	35	$2^4 \cdot 7^2 \cdot 11^4$
35	1	$2^4 \cdot 7 \cdot 11$	1365	15	$2^7 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11$
35	3	$2^8 \cdot 7$	1645	5	$2^7 \cdot 5^2 \cdot 7 \cdot 11^2$
37	3	$2^4 \cdot 11^2$	2099	21	$2^{19} \cdot 11$
45	5	$2^8 \cdot 5^2$	2373	9	$2^{13} \cdot 3^2 \cdot 7 \cdot 11$
49	5	$2^3 \cdot 7 \cdot 11^2$	2405	25	$2^8 \cdot 5^2 \cdot 11^3$
51	3	$2^5 \cdot 3^2 \cdot 11$	3507	21	$2^8 \cdot 3^2 \cdot 7^2 \cdot 11^2$
53	1	$2^8 \cdot 11$	6195	21	$2^{13} \cdot 3^2 \cdot 7^2 \cdot 11$
67	7	$2^4 \cdot 11^3$	6195	45	$2^5 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11^3$
69	9	$2^9 \cdot 3^2 \cdot 11$	6685	35	$2^{12} \cdot 5^2 \cdot 7^2 \cdot 11$
75	1	$2^9 \cdot 11$	6853	55	$2^{17} \cdot 7 \cdot 11^2$
83	5	$2^{10} \cdot 11$	6965	65	$2^{13} \cdot 5^2 \cdot 7 \cdot 11^2$
91	7	$2^9 \cdot 7^2$	8427	15	$2^{16} \cdot 3^2 \cdot 11^2$
91	9	$2^6 \cdot 7 \cdot 11^2$	9461	95	$2^8 \cdot 11^5$
93	3	$2^{10} \cdot 3^2$	16653	51	$2^5 \cdot 3^2 \cdot 7 \cdot 11^5$
105	5	$2^3 \cdot 5^2 \cdot 7 \cdot 11$	21399	63	$2^3 \cdot 3^2 \cdot 7^2 \cdot 11^5$
115	5	$2^6 \cdot 5^2 \cdot 11$	2865765	345	$2^{15} \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11^5$
133	7	$2^6 \cdot 7^2 \cdot 11$	11776659	795	$2^{30} \cdot 3^2 \cdot 11^4$

Table 1

Theorem 1. *All minimal positive integer solutions* (x, y, k) *to equation* (1.4)*, with* k *is divisible only by primes less than* 12*, are given in Table 1.*

2. An approach via integer points on elliptic curves

Suppose that (x, y, k) is a minimal solution to equation (1.4). Then $d = \gcd(x, y)$ is a squarefree positive integer, and either k is divisible only by $2, 7, 11$, or such an integer times one of $9, 25$ or 225, depending on whether $3, 5$ or 15 divides d respectively. Let $k = k_1 z^4$, where k_1 is 4th-power free. Then (x, y, z) satisfies

$$x^2 + 7y^4 = k_1 z^4.$$

Let $x = ud$ and $y = vd$, then d^2 divides k_1, and upon putting $k_2 = k_1/d^2$, we see that (u, v, k_2) satisfy

$$u^2 + 7d^2v^4 = k_2 z^4,$$

and so $(X, Y) = (u/z^2, v/z)$ is a $\{2, 7, 11, \infty\}$-integral point on the elliptic curve

$$\mathrm{E}_{d,k_2} : Y^2 = -7d^2X^4 + k_2. \tag{2.1}$$

It is easy to verify that $\gcd(d, k_2) = 1$, therefore solving (1.4) reduces to finding all S-integral points on all curves of the form in (2.1), where $S = \{2, 7, 11, \infty\}$, d runs over all positive squarefree integers divisible only by primes less than 12, and k_2 runs over all 4th-power free integers divisible only by primes less than 12, and coprime to d. Furthermore, it is easy to see that we can restrict to those values of k_2 for which $\mathrm{ord}_7\, k_2 \in \{0, 1\}$, and divisible only by 2, 7 and 11. There are a total of 300 such curves.

Pethő, Zimmer, Gebel and Herrmann [15] have recently described an algorithm[1] based on estimates for linear forms in elliptic logarithms, together with lattice basis reduction techniques, to determine all S-integer points on elliptic curves. Using these methods, we obtain the following result, from which Theorem 1 is an immediate consequence.

[1]This algorithm was implemented by the first author of the present paper and is part of the computer algebra system Magma [4].

Remark 2. There is a simple (non-birational) connection between equation (1.4) and an elliptic curve in canonical form. Assuming $y \neq 0$ we may multiply (1.4) by $(7y)^2$ and set $X = -7y^2$ and $Y = 7xy$. This gives the curve $Y^2 = X^3 - 7kX$. In the next section we shall present an algorithm to compute all S-integral points on an elliptic curve in canonical form which may be used to compute all S-integral solutions of equation (1.4).

3. Computing S-integral points on an elliptic curve

Let S denote a finite set of rational primes which includes the prime at infinity, and put $s = |S|$. To avoid technical difficulties, we assume that the elliptic curve is given by the short Weierstrass model

$$\mathcal{E}' : y^2 = x^3 + Ax + B, \quad (A, B \in \mathbb{Z}), \tag{3.1}$$

which is minimal for every prime in S. For the general case, we refer to the paper [15].

To apply the algorithm, it is necessary to assume that we can compute the Mordell–Weil group

$$\mathcal{E}(\mathbb{Q}) = \langle P_1 \rangle \times \cdots \times \langle P_r \rangle \times \mathcal{E}_{\mathrm{tors}}(\mathbb{Q}),$$

where $\mathcal{E}_{\mathrm{tors}}(\mathbb{Q})$ denotes the torsion group of finite order, say g. Let $\hat{h}$ denote the Néron–Tate height on $\mathcal{E}(\mathbb{Q})$, and let λ denote the smallest eigenvalue of the positive definite regulator matrix $(\hat{h}(P_i, P_j))_{1 \leq i, j \leq r}$.

Let $\wp(u)$ be the Weierstrass $\wp$-function corresponding to the curve $\mathcal{E}(\mathbb{C})$. Let $\Omega = \langle \omega_1, \omega_2 \rangle$ be its fundamental lattice, and ω_1 its real period. There exists, for any $P = (x, y) \in \mathcal{E}(\mathbb{C})$, an element $u \in \mathbb{C}/\Omega$, such that $(x, y) = (\wp(u), \frac{1}{2}\wp'(u))$. This is called the (complex) elliptic logarithm of P. In the sequel, $u_{i,\infty}$ denotes the elliptic logarithm of P_i for $i = 1, \ldots r$. We put $u'_{i,\infty} = g\frac{u_{i,\infty}}{\omega_1}$.

For a prime $q \in S$, let $\mathcal{E}_0(\mathbb{Q}_q)$ denote the points of $\mathcal{E}(\mathbb{Q}_q)$ with non-singular reduction modulo q. Then, by the assumption that equation (3.1) is minimal at q, the index $[\mathcal{E}(\mathbb{Q}_q) : \mathcal{E}_0(\mathbb{Q}_q)]$ is finite, and equal to the Tamagawa number c_q. Let $\tilde{\mathcal{E}}$ denote the reduced curve $\mathcal{E}$ modulo q, and let $\mathcal{N}_q = \#\tilde{\mathcal{E}}(\mathbb{F}_q)$ be the number of rational points of $\tilde{\mathcal{E}}/\mathbb{F}_q$. With g being the order of the torsion group, we define the number

$$m = m_q = \operatorname{lcm}(\operatorname{lcm}(2, g), c_q \cdot \mathcal{N}_q).$$

Finally, for the finite places $q \in S$, let $q'_{i,q}$ denote the q-adic elliptic logarithm of mP_i for $i = 1, \ldots, r$. For the definition and basic properties of q-adic elliptic logarithms, we refer the reader to [17], and to [15].

Denote by P an S-integral point on $\mathcal{E}$. P can be expressed in the form

$$P = \sum_{i=1}^{r} n_i P_i + T \tag{3.2}$$

for a suitable torsion point T. Using the main result from [15], we get an upper bound N for $|n_i|$, and we know that there is a prime $q \in S$ for which the inequality

$$\Big| \sum_{i=1}^{r} n_i u'_{i,q} + n_{r+1} \Big|_q \leq c_5 \exp\{-(\lambda/s)N^2 + c_2/s\},$$

holds. Here, c_2, c_5 and N are explicit constants which can be found in [15]. The last inequality defines a diophantine approximation problem which can be solved by using LLL-reduction, as described in [18]. The reduction technique is applied several times until the value of N cannot be reduced any further. With a small enough value for N, one checks all linear combinations in (3.2), with $|n_i| \leq N$, thereby producing all S-integral solutions on the elliptic curve.

To demonstrate the method, we consider the quartic elliptic equation

$$\mathcal{Q} : y^2 = -7x^4 + 11,$$

with $S = \{2, 7, 11, \infty\}$. In order to obtain an elliptic curve in Weierstrass form, we multiply by $49x^2$ and set

$$X = -7x^2 \quad \text{and} \quad Y = 7xy.$$

This leads to the curve

$$\mathcal{E} : Y^2 = X^3 - 77X.$$

Since every S-integral point on $\mathcal{Q}$ will be S-integral on $\mathcal{E}$, we may apply the method described above. We note that the transformation between $\mathcal{Q}$ and $\mathcal{E}$ is not an isomorphism between the curves.

Using the program MWRANK [20], we obtain that the rank of the curve is 2, and the two generators of the free part of the abelian group are

$$P_1 = (-7, 14), \quad P_2 = (9, 6).$$

The generator of the torsion subgroup is $T = (0, 0)$, which is of order 2. It is easy to check that $\mathcal{E}$ is minimal for every finite prime $p \in S$, hence we can use the estimates for the value N from [15]. In so doing, we find that $N = 1.64 \cdot 10^{123}$. We now construct linear forms in complex and p-adic elliptic logarithms following the description in [15]. Applying several times an LLL-reduction procedure to these linear forms leads eventually to the smaller value $N = 5$. Finally, computing all linear combinations $n_1P_1 + n_2P_2 + n_3T$ for $n_1 = 0, \ldots, 5$, $|n_2| \leq 5$ and $n_3 = 0, 1$, we get the points $(X, |Y|) \in \mathcal{E}(\mathbb{Z}_S)$:

$$(0,0),\ (9,6),\ (176,2332),\ (-7,14),\ (44,-286),\ (11,22), (-7/4,91/8),$$
$$(-7/16,371/64),\ (81/4,657/8),\ (-63175/7744,6291565/681472).$$

Mapping these points back to $\mathcal{Q}$ shows that the only S-integral solutions of $\mathcal{Q}$ are the tuples $(|x|, |y|)$ given by

$$(1,2),\ (1/2,13/4),\ (1/4,53/16),\ (95/88,9461/7744).$$

References

[1] M. Bauer and M. A. Bennett, Applications of the hypergeometric method to the generalized Ramanujan–Nagell equation, 2001, (preprint).

[2] F. Beukers, On the generalized Ramanujan–Nagell equation I., *Acta Arith.* **38** (1980), 389–410.

[3] F. Beukers, On the generalized Ramanujan–Nagell equation II., *Acta Arith.* **39** (1981), 113–123.

[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comp.* **24** 3/4 (1997), 235–265, (See also the Magma home page at http://www.maths.usyd.edu.au:8000/u/magma/).

[5] E. L. Cohen, On the Ramanujan–Nagell equation and its generalizations, Number Theory (Banff, AB, 1988), *de Gruyter*, *Berlin*, 1990, 81–92.

[6] W. Ljunggren, Einige Eigenschaften der Einheiten reeller quadratischer und rein-biquadratischer Zahl-Körper usw., *Oslo Vid.-Akad. Skrifter*, no. 12 (1936).

[7] W. Ljunggren, Über die unbestimmte Gleichung $Ax^2 - By^4 = C$, *Arch. for Mathematik og Naturvidenskab* **41**, no. 10 (1938).

[8] W. Ljunggren, Über die Gleichung $x^4 - Dy^2 = 1$, *Arch. Math. Naturv.* **45**, no. 5 (1942).

[9] W. Ljunggren, Ein Satz über die Diophantische Gleichung $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$, Tolfte Skand. Matemheikerkongressen, Lund, 1953, 1954, 188–194.

[10] W. Ljunggren, On the Diophantine equation $Ax^4 - By^2 = C$ $(C = 1, 4)$, *Math. Scand.* **21** (1967), 149–158.

[11] K. Mahler, On the greatest prime factor of $ax^m + by^n$, *Nieuw Arch. Wiskd.*, III., Ser. **1** (1953), 113–122.

[12] L. J. Mordell, Diophantine Equations, *Academic Press*, *New York*, 1969.

[13] T. Nagell, The diophantine equation $x^2 + 7 = 2^n$, *Arkiv matematik* **4** (1960), 185–187.

[14] A. Pethő and B. M. M. de Weger, Products of prime powers in binary recurrence sequences, *Report of the Math. Inst. Univ. Leiden*, 1985.

[15] A. Pethő, H. Zimmer, J. Gebel and E. Herrmann, Computing all S-integral points on elliptic curves, *Proc. Camb. Phil. Soc.* **127** (1999), 1–23.

[16] S. V. Kotov, Über die maximale Norm der Idealteiler des Polynoms $\alpha x^m + \beta y^n$ mit den algebraischen Koeffizienten, *Acta Arith.* **31** (1976), 219–230.

[17] J. H. Silverman, The Arithmetic of Elliptic Curves, *Graduate Texts in Math.* **106**, *Springer-Verlag, New York*, 1986.

[18] B. M. M. de Weger, Algorithms for diophantine equations, Ph.D. Thesis, Centr. for Wiskunde en Informatica, *Amsterdam*, 1987.

[19] P. G. Walsh, Diophantine equations of the form $aX^4 - bY^2 = \pm 1$, in: Algebraic Number Theory and Diophantine Analysis, Proceedings of a conference in Graz 1998, (F. Halter-Koch and R. Tichy, eds.), de Gruyter Proceedings in de Gruyter, 2000.

[20] MWRANK, A package to compute ranks of elliptic curves,
http://www.maths.ott.ac.uk/personal/jec/ftp/progs.

E. HERRMANN
FR 6.1 MATHEMATIK
UNIVERSITÄT DES SAARLANDES
POSTFACH 151150
D-66041 SAARBRÜCKEN
GERMANY

E-mail: herrmann@math.uni-sb.de

F. LUCA
INSTITUTO DE MATEMÁTICAS UNAM
CAMPUS MORELIAAP. POSTAL 61-3 (XANGARI)CP 58 089
MORELIA, MICHOACÁN
MEXICO

E-mail: fluca@matmor.unam.mx

P. G. WALSH
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF OTTAWA
585 KING EDWARD ST.
OTTAWA, ONTARIO, K1N-6N5
CANADA

E-mail: gwalsh@mathstat.uottawa.ca

(Received July 27, 2002; revised May 12, 2003)