Yet another generalization of the Ramanujan-Nagell equation

M.A. Bennett, M. Filaseta and O. Trifonov

March 12, 2007

1 Introduction

An old problem of Ramanujan, solved first by Nagell [11], amounts to showing that the Diophantine equation

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

has only the solutions in integers corresponding to $n = 3, 4, 5, 7$ and 15. This rather curious seeming equation arises in a variety of settings, ranging from coding theory to the classification of finite simple groups; surveys of work in this area can be found in [8] and [1]. Numerous generalizations of this problem may be found in the literature. Among the more recent along these lines, we mention papers of Bugeaud, Mignotte and Siksek [7] and Herrmann, Luca and Walsh [9], where equations of the shape

$$x^2 + 7 = y^n \quad \text{and} \quad x^2 + 7y^4 = 2^{n_1}7^{n_2}11^{n_3},$$

respectively, are solved completely.

In this paper, we will present a rather different generalization of the equation of Ramanujan-Nagell. Specifically, we prove

Theorem 1.1. *If x, n and m are positive integers satisfying*

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

then either $x \in \{1, 3, 5, 11, 181\}$ or $m > x^{1/2}$.

Our approach will be via a nontraditional application of the hypergeometric method of Thue and Siegel, where we utilize rational function approximation to the binomial function, evaluated at integers in an imaginary quadratic field. This, while combining some of the ingredients from earlier work of Beukers [5], [6], is fundamentally quite different. Indeed, it is more in the spirit of recent work of the authors [3], based upon approximation to the binomial function with integral exponents, unlike that considered in [5] and [6]. In [3], one finds, by way of example, lower bounds of the shape $m > x^{0.285}$ upon integer m satisfying

$$x^2 + x = 2^j 3^k m,$$

with $x > 8$ integral and $j, k \in \mathbb{Z}$. Theorem 1.1 treats a somewhat similar situation where the primes $p = 2$ and $q = 3$ are replaced by $p = (1+\sqrt{-7})/2$ and $q = (1-\sqrt{-7})/2$.

Given $\epsilon > 0$, it is possible (see e.g [10]) to obtain a lower bound for m in equation (1.1) of the shape $m > x^{1-\epsilon}$, valid for suitably large x. Quantifying such an ineffective statement, however, is a notoriously difficult problem in Diophantine approximation. It is easy to show that there exist infinitely many triples of positive integers (x, m, n) satisfying (1.1) with $m < x$.

2 Padé Approximants

Before we proceed with our proof, we need to state some basic results from the theory of (diagonal) Padé approximation to the binomial function $(1-x)^k$, for k integral. For our purposes, either [2] or [4] is a viable source; therein we find the following:

Lemma 2.1. *Let k and r be positive integers with $k > r$. There exist polynomials $P_r(x)$, $Q_r(x)$, and $E_r(x)$ in $\mathbb{Z}[x]$ satisfying:*

(i) $$Q_r(x) = \frac{(k+r)!}{(k-r-1)!\,r!\,r!} \int_0^1 (1-t)^r t^{k-r-1} (1-t+xt)^r \, dt$$

(ii) $$E_r(x) = \frac{(k+r)!}{(k-r-1)!\,r!\,r!} \int_0^1 (1-t)^r t^r (1-tx)^{k-r-1} \, dt$$

(iii) $\deg P_r = \deg Q_r = r$ *and* $\deg E_r = k-r-1$

(iv) $P_r(x) - (1-x)^k Q_r(x) = (-1)^r x^{2r+1} E_r(x)$

(v) $P_r(x)Q_{r+1}(x) - Q_r(x)P_{r+1}(x) = cx^{2r+1}$ *for some non-zero constant* c.

As is perhaps somewhat traditional, at this stage it is worth noting that the quantity of importance here is the ratio k/r, which must be tailored to the problem at hand. For our purposes, here and henceforth we will take

$$k = 5j, \;\; r = 4j - \delta \;\text{ and }\; x_0 = \frac{7 + 181\sqrt{-7}}{2^{14}}, \tag{2.1}$$

where $\delta \in \{0, 1\}$ and j is a positive integer. For later use, we require bounds upon $|E_r(x_0)|$ and $|Q_r(x_0)|$:

Lemma 2.2. *If* j *is a positive integer,* $\delta \in \{0, 1\}$*, and* k, r *and* x_0 *are as in (2.1), then we have*

$$|Q_r(x_0)| < 0.31 \times 256.07^j \quad \textit{and} \quad |E_r(x_0)| < 0.22 \times 23.1^j.$$

Proof. We will present the proof for $\delta = 0$; the case $\delta = 1$ is similar. From Lemma 4 of [2], we have that

$$\frac{(k+r)!}{(k-r-1)!\,r!\,r!} = \frac{(9j)!}{(j-1)!((4j)!)^2} < \frac{3}{8\pi}\left(3^{18}2^{-16}\right)^j.$$

Since we have, for $t \in [0, 1]$,

$$|1 - (1 - x_0)t|^2 = 1 - \frac{16377}{8192}t + t^2$$

and since

$$\max_{t\in[0,1]} \left\{(1-t)^4 t \left(1 - \frac{16377}{8192}t + t^2\right)^2\right\} = 0.04331533667\ldots,$$

it follows that

$$\begin{aligned}
&\left| \int_0^1 (1-t)^r t^{k-r-1}(1 - t + x_0 t)^r \,\mathrm{d}t \right| \\
&\quad \le \int_0^1 \left((1-t)^4 t\left(1 - \frac{16377}{8192}t + t^2\right)^2\right)^{j-1} (1-t)^4\left(1 - \frac{16377}{8192}t + t^2\right)^2 \mathrm{d}t \\
&\quad < 0.0433154^{j-1} \int_0^1 (1-t)^4\left(1 - \frac{16377}{8192}t + t^2\right)^2 \mathrm{d}t \\
&\quad < 2.566 \times 0.0433154^j.
\end{aligned}$$

We deduce that

$$|Q_r(x_0)| < 0.31 \cdot 256.07^j.$$

From the fact that $t \in [0,1]$ implies

$$|1 - tx_0|^2 = 1 - \frac{7}{8192}t(1-t) \leq 1,$$

we have

$$\left| \int_0^1 (1-t)^r t^r (1-tx_0)^{k-r-1} \, \mathrm{d}t \right| \leq \int_0^1 (1-t)^r t^r \, \mathrm{d}t < 256^{-j}$$

and hence

$$|E_r(x_0)| < \frac{3}{8\pi} \left(3^{18} 2^{-24}\right)^j < \frac{3}{8\pi} \times 23.1^j.$$

The choice $\delta = 1$ leads to a stronger upper bound for $|Q_r(x_0)|$ and the slightly weaker stated inequality for $|E_r(x_0)|$. □

As a final note before we proceed, applying Lemma 1 of [2] or Lemma 3.1 of [3], with our slight variation in notation, we may write

$$P_r(x) = (-1)^\delta \sum_{i=0}^{4j-\delta} \binom{9j-\delta}{i} \binom{8j-2\delta-i}{4j-\delta} (-x)^i$$

and

$$Q_r(x) = \sum_{i=0}^{4j-\delta} \binom{8j-2\delta-i}{4j-\delta} \binom{j+\delta-1+i}{i} x^i.$$

Defining

$$\mathcal{G}_\delta(j) = \gcd_{i \in \{0,1,\ldots,4j-\delta\}} \left(\binom{8j-2\delta-i}{4j-\delta} \binom{j+\delta-1+i}{i} \right),$$

it is clear that $\mathcal{G}_\delta(j)^{-1} Q_r(x) \in \mathbb{Z}[x]$. As a consequence of Lemma 2.1 (iv), we also have that $\mathcal{G}_\delta(j)^{-1} P_r(x)$ and $\mathcal{G}_\delta(j)^{-1} E_r(x)$ are in $\mathbb{Z}[x]$. A special case of Proposition 5.1 of [3] leads to the following

Lemma 2.3. *If $j > 50$ is an integer and $\delta \in \{0,1\}$, then*

$$\mathcal{G}_\delta(j) > 2.943^j.$$

3 Proof of Theorem 1.1 for Large n

Let us assume that x, n and m are positive integers satisfying (1.1) with, say,

$$n > 4000 \quad \text{and} \quad m \le x^{1/2}. \tag{3.1}$$

Write

$$\alpha = \frac{1+\sqrt{-7}}{2}, \ \ \beta = \alpha^{13} = \frac{-181-\sqrt{-7}}{2},$$

and $\gamma = \beta - \overline{\beta}$ (so that $x_0 = \gamma/\beta$). The ring $R = \mathbb{Z}[(1+\sqrt{-7})/2]$ is the ring of algebraic integers in $\mathbb{Q}(\sqrt{-7})$. It is a Unique Factorization Domain, so that primes and irreducibles are the same in R. We observe that

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right) = \left(\frac{1+\sqrt{-7}}{2}\right)^{n-2}\left(\frac{1-\sqrt{-7}}{2}\right)^{n-2} m, \tag{3.2}$$

where each factor is in R, and $(1+\sqrt{-7})/2$ and $(1-\sqrt{-7})/2$ are primes in R. The difference of the two factors on the left of (3.2) is $\sqrt{-7}$ which has norm 7. Since $\alpha\overline{\alpha} = 2$, it follows that the two factors cannot both be divisible by α and that they cannot both be divisible by $\overline{\alpha}$. Furthermore, since the two factors on the left of (3.2) are conjugates, if one is divisible by α, then the other is divisible by $\overline{\alpha}$. We deduce that for some positive integer j and, hence, $k = 5j$ chosen appropriately, there is a μ in R such that

$$\beta^k\mu - \overline{\beta}^k\overline{\mu} = \pm\sqrt{-7}. \tag{3.3}$$

Here, $\mu\overline{\mu} = 2^\ell m$ where $0 \le \ell \le 64$; in particular, $\mu \ne 0$. Also,

$$|\beta^k\mu| = \sqrt{\frac{x^2+7}{2}} > 0.7 \cdot x.$$

Note that the first inequality in (3.1) implies that $j \ge 61$ and $k \ge 305$. Furthermore, as $x^2 + 7 = 2^n m \ge 2^n$, we see that $x > 2^{2000}$.

In essence what equation (3.3) tells us is that the quotient $(\beta/\overline{\beta})^k$ is well approximated by an algebraic number with, provided m is small, rather modest height. We will use the hypergeometric method to deduce that, since such an event occurs rather dramatically for $k = 1$, it cannot remain the case for larger k.

We use the polynomials of Lemma 2.1, after dividing by $\mathcal{G}_\delta(j)$. Specifically, define

$$P_r^*(x) = \mathcal{G}_\delta(j)^{-1} P_r(x), \;\; Q_r^*(x) = \mathcal{G}_\delta(j)^{-1} Q_r(x)$$

and

$$E_r^*(x) = \mathcal{G}_\delta(j)^{-1} E_r(x),$$

recalling that they have rational integer coefficients. Observe that $x_0 = \gamma/\beta$ and (iii) of Lemma 2.1 imply $\beta^r P_r^*(x_0)$, $\beta^r Q_r^*(x_0)$, and $\beta^{k-r-1} E_r^*(x_0)$ are in R. From (iv) of Lemma 2.1 and multiplying through by β^{r+k}, we obtain

$$\beta^k P - \overline{\beta}^k Q = E, \tag{3.4}$$

where

$$P = \beta^r P_r^*(x_0), \quad Q = \beta^r Q_r^*(x_0), \quad \text{and} \quad E = (-1)^r \beta^{k-r-1} \gamma^{2r+1} E_r^*(x_0)$$

are in R.

Multiplying both sides of (3.3) by Q and both sides of (3.4) by $\overline{\mu}$ and subtracting, we obtain

$$\beta^k \big(Q\mu - P\overline{\mu}\big) = \pm Q \cdot \sqrt{-7} - E\overline{\mu}.$$

Note that part (v) of Lemma 2.1 implies, for one of $r = 4j$ or $4j-1$, the expression on the left is non-zero. If $a + b\sqrt{-7} \in R$ (so a and b are half-integers and $a + b \in \mathbb{Z}$), then $|a + b\sqrt{-7}| = \sqrt{a^2 + 7b^2}$. It follows that $|Q\mu - P\overline{\mu}| \geq 1$. Thus,

$$|\beta|^k \leq |Q| \cdot \sqrt{7} + |E||\overline{\mu}|.$$

This is our fundamental inequality; upper bounds upon $|Q|$ and $|E|$ lead to a corresponding lower bound for $|\mu|$ and hence m. From Lemmata 2.2 and 2.3, we obtain

$$|Q| \cdot \sqrt{7} < \left(5.84 \cdot 10^9\right)^j.$$

As $j \geq 18$ and $|\beta|^k > (6.07 \cdot 10^9)^j$, we deduce $|Q| \cdot \sqrt{7} < |\beta|^k/2$. Hence,

$$\frac{1}{2} \cdot |\beta|^k \leq |\beta|^{k-r-1} |\gamma|^{2r+1} |E_r^*(x_0)||\mu|. \tag{3.5}$$

Observe that

$$\frac{|\beta|^{r+1}}{|\gamma|^{2r+1}} \geq 2.64 \cdot 27950^j \quad \text{and} \quad |E_r^*(x_0)| \leq 0.22 \cdot 7.85^j,$$

where the latter inequality is a consequence of Lemmata 2.2 and 2.3. Hence,

$$|\mu| \geq 6 \cdot 3560^j.$$

One checks that

$$(|\beta|^k)^{0.363} = (|\beta|^{5 \cdot 0.363})^j < 3560^j.$$

We deduce that

$$|\mu|^{1.363} \geq 6 \cdot 3560^j \cdot \frac{(|\beta|^k)^{0.363}}{3560^j} \cdot |\mu|^{0.363} \geq 6(|\beta|^k|\mu|)^{0.363} > x^{0.363}.$$

As $x > 2^{2000}$, we obtain

$$m \geq \frac{|\mu|^2}{2^{64}} > \frac{x^{0.532}}{2^{64}} > \sqrt{x},$$

contradicting (3.1).

4 Final computations

To complete the proof of Theorem 1.1, it remains to show that solutions to equation (1.1) with $n \notin \{3, 4, 5, 7, 15\}$ and $n \leq 4000$ necessarily have $m > x^{1/2}$. This is obviously a finite computation, but it is worth observing that it can in fact be carried out rather quickly. For a fixed choice of n in the interval of interest, the idea is to look at the solutions of

$$x^2 + 7 \equiv 0 \pmod{2^n}.$$

For $n \geq 3$, there are four in the interval $[1, 2^n - 1]$, and these are the only ones we need consider. For each such solution x_0, we can simply check if $m = (x_0^2 + 7)/2^n$ satisfies $m < x^{1/2}$. However, computing the roots of $x^2 + 7 \equiv 0 \pmod{2^n}$ for each n is unnecessary, and a program can be sped up as follows. One keeps track of only two of the solutions for a given n, say $x_1 = x_1(n)$ and $x_2 = x_2(n)$, having the property that $(x_j^2 + 7)/2^n$ is odd for $j \in \{1, 2\}$. That two and only two such solutions exist in $[1, 2^n - 1]$ can

be established by induction. Indeed, if it is true for some n, note that each $x_j(n)$ is odd and the numbers

$$y_1 = x_1(n) + 2^{n-1}, \quad y_2 = x_1(n) - 2^{n-1},$$
$$y_3 = x_2(n) + 2^{n-1}, \quad y_4 = x_2(n) - 2^{n-1}$$

are four incongruent solutions to $x^2 + 7 \equiv 0 \pmod{2^{n+1}}$. Also, $(y_1^2 + 7) - (y_2^2 + 7)$ and $(y_3^2 + 7) - (y_4^2 + 7)$ are odd multiples of 2^{n+1} so that exactly one of $y_1^2 + 7$ and $y_2^2 + 7$ is divisible by 2^{n+2} and exactly one of $y_3^2 + 7$ and $y_4^2 + 7$ is divisible by 2^{n+2}. Thus, we can compute $x_1(n+1)$ by determining which of $y_1^2 + 7$ and $y_2^2 + 7$ is not divisible by 2^{n+2} and similarly compute $x_2(n+1)$ by determining which of $y_3^2 + 7$ and $y_4^2 + 7$ is not divisible by 2^{n+2}. In this manner, we are able to show that $m < x^{1/2}$ for each $n \notin \{3, 4, 5, 7, 15\}$ with $n \leq 4000$, completing the proof of Theorem 1.1.

5 Concluding remarks

The machinery we have presented here can be used with slightly more effort to sharpen Theorem 1.1 to deduce an inequality of the shape $m > x^{0.566}$ for suitably large x (where this statement can be made explicit). We will not undertake this here. Additionally, similar arguments lead to results for equations of the shape $x^2 + 4 = 5^n m$, for instance, where the analog of the identity $181^2 + 7 = 2^{15}$ is provided by $11^2 + 4 = 5^3$.

References

[1] M. Bauer and M. A. Bennett, *Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation*, Ramanujan J. 6 (2002), no. 2, 209–270.

[2] M. Bennett, *Fractional parts of powers of rational numbers*, Math. Proc. Cambridge Philos. Soc. 114 (1993), no. 2, 191–201.

[3] M. Bennett, M. Filaseta and O. Trifonov, *On the factorization of consecutive integers*, submitted for publication.

[4] F. Beukers, *Fractional parts of powers of rationals*, Math. Proc. Cambridge Philos. Soc. 90 (1981), no. 1, 13–20.

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

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

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

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

[9] E. Herrmann, F. Luca and P. G. Walsh, *A note on the Ramanujan-Nagell equation*, Publ. Math. Debrecen 64 (2004), no. 1-2, 21–30.

[10] K. Mahler, Lectures on Diophantine Approximations I, University of Notre Dame, 1961.

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