Glasgow Math. J. **61** (2019) 535–544. © Glasgow Mathematical Journal Trust 2018.
doi:10.1017/S0017089518000344.

A GENERALIZATION OF THE RAMANUJAN–NAGELL EQUATION

TOMOHIRO YAMADA
Center for Japanese Language and Culture,
Osaka University,
8-1-1, Aomatanihigashi, Minoo, Osaka 562-8558, Japan
e-mail: tyamada1093@gmail.com

(Received 7 February 2018; revised 27 June 2018; accepted 17 July 2018
first published online 22 August 2018)

Abstract. We shall show that, for any positive integer $D > 0$ and any primes p_1, p_2, the diophantine equation $x^2 + D = 2^s p_1^k p_2^l$ has at most 63 integer solutions (x, k, l, s) with $x, k, l \geq 0$ and $s \in \{0, 2\}$.

1991 *Mathematics Subject Classification.* Primary 11D61, Secondary 11D45.

1. Introduction. It is known that the equation $x^2 + 7 = 2^n$ has five solutions, as conjectured by Ramanujan and shown by Nagell [**26**] and other authors. According to this history, this diophantine equation has been called the Ramanujan–Nagell equation and several authors have studied various analogues.

Apéry [**1**] showed that, for each integer $D > 0$ and prime p, the equation $x^2 + D = p^n$ has at most two solutions unless $(p, D) = (2, 7)$ and, for any odd prime p, the equation $x^2 + D = 4p^n$, which is equivalent to $y^2 + y + (D + 1)/4 = p^n$ with y odd, also has at most two solutions. Beukers [**5**] showed that if $D > 0$ and $x^2 + D = 2^n$ has two solutions, then $D = 23$ or $D = 2^k - 1$ for some $k > 3$ and also gave an effective upper bound: if $w = x^2 + D = 2^n$ with $D \neq 0$, then $w < 2^{435} |D|^{10}$.

Further generalizations have been made by Le [**18–20**], Skinner [**29**] and Bender and Herzberg [**2**] to prove that, for any given integers A, B, s, p with $\gcd(A, B) = 1$, $s \in \{0, 2\}$ and p prime, $Ax^2 + B = 2^s p^n$ has at most two solutions except $2x^2 + 1 = 3^k$, $3x^2 + 5 = 2^k$, $x^2 + 11 = 4 \times 3^k$, $x^2 + 19 = 4 \times 5^k$ with three solutions and the Ramanujan–Nagell one $x^2 + 7 = 2^k$ with five solutions.

Bender and Herzberg [**2**] also found some necessary conditions for the equation $D_1 x^2 + D_2 = 2^s a^n$ with $D_1 > 0$, $D_2 > 0$, $\gcd(D_1, D_2) = \gcd(D_1 D_2, k) = 1$, $s \in \{0, 2\}$ to have more than $2^{\omega(a)}$ solutions. With the aid of the primitive divisor theorem of Bilu, Hanrot and Voutier [**7**] concerning Lucas and Lehmer sequences, Bugeaud and Shorey [**10**] determined all instances for which $D_1 x^2 + D_2 = 2^m a^n$ with $D_1 > 0$, $D_2 > 0$, $\gcd(D_1, D_2) = \gcd(D_1 D_2, k) = 1$, $m \in \{0, 1, 2\}$ has more than $2^{\omega(a)-1}$ solutions, although they erroneously refer to $2x^2 + 1 = 3^n$ as it has just two solutions $n = 1, 2$, which in fact has exactly three solutions $n = 1, 2, 5$, as pointed out by Leu and Li [**23**] (this fact immediately follows from Ljunggren's result [**24**] since $2x^2 + 1 = 3^n$ is equivalent to $(3^n - 1)/2 = x^2$).

We note that it is implicit in Le [**15**] that if $D_1 > 3$, then $D_1 x^2 + 1 = p^n$ has at most one solution except $(D_1, p) = (7, 2)$. But it is erroneously cited in another work of Le [**21**], stating that $D_1 x^2 + 1 = p^n$ has at most one solution for each $D_1 \geq 1$ and odd prime p. This may have caused the failure in [**10**] mentioned above.

Le [16] studied another generalized Ramanujan–Nagell equation $x^2 + D^m = p^n$ with $m, n, x > 0$, p a prime not dividing D to show that this equation has at most two solutions except for some special cases. Further studies by Bugeaud [8] and Yuan and Hu [33] concluded that this equation has at most two solutions except for $(D, p) = (7, 2), (2, 5)$ and $(4, 5)$, in which cases, this equation has, respectively, exactly six, three and three. Hu and Le [14] showed that, for integers $D_1, D_2 > 1$ and a prime p not dividing D_1D_2, the equation $D_1x^2 + D_2^m = p^n$, $x, m, n > 0$ has at most two solutions except for $(D_1, D_2, p) = (2, 7, 13), (10, 3, 13), (10, 3, 37)$ and $((3^{2l} - 1)/a^2, 3, 4 \times 3^{2l-1} - 1)$ with $a, l \geq 1$, in which cases this equation has exactly three solutions.

The diophantine equation $x^2 + D = y^n$ with only D given also has been studied. Lebesgue [22] solved this equation for $D = 1$, Nagell solved for $D = 3$ and Cohn [11] solved for many values of D. By the theorem of Shorey, van der Poorten, Tijdeman and Schinzel [28], we have $x, y, n \leq C$ with an effectively computable constant C depending only on D. Combining a modular approach developed by Taylor and Wiles [31, 32] and Bennett and Skinner [3] and other methods, Bugeaud, Mignotte and Siksek [9] solved $x^2 + D = y^n$ in (x, y, n) with $n \geq 3$ for each $1 \leq D \leq 100$. Furthermore, Le [17] showed that if $x^2 + 2^m = y^n$ with $m, x > 0$, $n > 2$ and y odd, then $(x, m, y, n) = (5, 3, 1, 3), (7, 3, 5, 4)$ or $(11, 5, 2, 3)$. Pink [27] solved $x^2 + D = y^n$, $n \geq 3$, $\gcd(x, y) = 1$ for $D = 2^a3^b5^c7^d$ except the case $D \equiv 7 \pmod 8$ and y is even. A brief survey on further results to such equations is given by Bérczes and Pink [4]. More recently, Godinho, Marques and Togbé [13] solved $x^2 + D = y^n$, $n \geq 3$, $\gcd(x, y) = 1$ for $D = 2^a3^b17^c$ and $D = 2^a13^b17^c$.

In this paper, we shall study another generalization of the Ramanujan–Nagell equation

$$x^2 + D = 2^s p_1^k p_2^l \tag{1}$$

with $s \in \{0, 2\}$.

Evertse [12] showed that for every nonzero integer D and r prime numbers $p_1, p_2, \ldots, p_r$, $x^2 + D = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ has at most $3 \times 7^{4r+6}$ solutions. Hence, (1) has at most 3×7^{14} solutions for any given D, p_1, p_2. The purpose of this paper is to improve this upper bound for the number of solutions of (1).

THEOREM 1.1. *For every positive integer D and primes p_1, p_2, (1) has at most* 63 *integral solutions* (x, s, k, l) *with* $k, l \geq 0, s \in \{0, 2\}$.

It seems that we cannot use the primitive divisor theory for such types of equations. Instead, we shall use Beukers' method. However, we need a more involved argument than Beukers' original argument in [5].

Let $P(x) = x^2 + D$. Hence, (1) can be rewritten as $P(x) = 2^s p_1^k p_2^l$. In order to extend Beukers' argument for (1), we shall divide the set of solutions of this equation. Let $S(\alpha, \alpha + \delta, X, Y) = S_{P(x)}(\alpha, \alpha + \delta, X, Y)$ be the set of solutions of the equation $P(x) = 2^s p_1^k p_2^l$ with $X \leq P(x) < Y$, $s \in \{0, 2\}$ and $(p_1^k p_2^l)^\alpha \leq p_1^k \leq (p_1^k p_2^l)^{\alpha+\delta}$ and we write $S(\alpha, \alpha + \delta) = S(\alpha, \alpha + \delta, 0, \infty)$ for brevity. Moreover, for $u, v \pmod 2$, let $S(\alpha, \alpha + \delta, X, Y; u, v) = S_{P(x)}(\alpha, \alpha + \delta, X, Y; u, v)$ be the set of solutions $x^2 + D = 2^s p^k q^l \in S(\alpha, \alpha + \delta, X, Y)$ with $k \equiv u \pmod 2$, $l \equiv v \pmod 2$ and $S(\alpha, \alpha + \delta; u, v) = S(\alpha, \alpha + \delta, 0, \infty; u, v)$. Finally, let us write $S(X, Y) = S(0, 1, X, Y)$, $S^{(j)} = S(j/4, (j + 1)/4, 0, \infty)$, $S^{(j)}(X, Y) = S(j/4, (j + 1)/4, X, Y)$ and $S^{(j)}(X, Y; u, v) = S(j/4, (j + 1)/4, X, Y; u, v)$ for $j = 0, 1, 2, 3$.

Now, we shall state our result in more detail.

THEOREM 1.2. *Let* $Y = 4883601$ *and* W *be the constant defined in Lemma 3.1 with* $\delta = 1/4$ *and* $\delta_1 = 0.04377667$. *Moreover, let* y_1 *be the smallest solution of (1). For every positive integer* D *and primes* $p_1 < p_2$, *we have the following:*

(*i*) *Each* $S^{(j)}(W, \infty; u, v)$ *contains at most three solutions for* $j = 1, 2$, *two solutions for* $j = 0, 3$ *and no solution for* $u \equiv v \equiv 0 \pmod 2$. *Hence, there exist at most* 30 *solutions with* $x^2 + D \geq W$.

(*ii*) *If* $D \geq Y$ *or* $y_1 \geq Y$, *then* $S^{(j)}(y_1, W)$ *contains at most nine solutions for* $j = 1, 2$ *and five solutions for* $j = 0, 3$. *Hence, there exist at most* 28 *solutions with* $x^2 + D < W$.

(*iii*) *If* $D, y_1, p_2 < Y$, *then there exist at most* 29 *solutions with* $x^2 + D < W$.

(*iv*) *If* $D, y_1 < Y < p_2$, *then* $S^{(j)}(Y, W)$ *contains at most nine solutions for* $j = 1, 2$ *and five solutions for* $j = 0, 3$. *Hence, there exist at most* 28 *solutions with* $Y \leq x^2 + D < W$. *Moreover, there exist at most five solutions with* $x^2 + D < Y$.

In the next section, we prove a weaker gap principle using only elementary argument using congruences, which is used to bound the number of middle solutions (and as an auxiliary tool to prove a stronger gap principle in Section 4). In Section 3, we use Beukers' argument to show that if we have one large solution $w = x^2 + D$ in a class $S^{(j)}(W, \infty; u, v)$, then other solutions in the same class as w must be bounded by w. Combining an gap argument proved in Section 4, we obtain an upper bound for the number of solutions in each class. The number of small solutions can be checked by computer search.

2. An elementary gap argument. In this section, we shall give the following two gap principles shown by elementary arguments using congruence.

LEMMA 2.1. *Let* $x_1 < x_2$ *be two integers such that* $y_i = x_i^2 + D (i = 1, 2)$ *belong to the same set* $S_{P(x)}(\alpha, \alpha + \delta)$, *where* α, δ *are two real numbers satisfying* $0 \leq \delta < 1/4$ *and* $\alpha = 0$ *or* $0 \leq \alpha \leq 1 \leq \alpha + \delta$. *Then, we have* $x_2 > \frac{1}{2}(P(x_1)/4)^{3/4}$.

Proof. Let $x_1 < x_2$ be two integers in $S_{P(x)}(3/4, 1)$. Then, we can easily see that $P(x_i) \equiv 0 \pmod{p_1^{e_i}}$ with $p_1^{e_i} \geq (P(x_1)/4)^{3/4}$. This implies that $P(x_1) \equiv P(x_2) \equiv 0 \pmod{p_1^f}$, where $f = \min\{e_1, e_2\}$. Hence, we have $x_1 + x_2 \geq p_1^f \geq (P(x_1)/4)^{3/4}$, and therefore $x_2 > \frac{1}{2}(P(x_1)/4)^{3/4}$. Similarly, if $x_1 < x_2$ are two integers in $S_{P(x)}(0, 1/4)$, then $x_2 > \frac{1}{2}(P(x_1)/4)^{3/4}$. This proves the lemma. □

LEMMA 2.2. *Let* $x_1 < x_2 < x_3$ *be three integers such that* $y_i = x_i^2 + D (i = 1, 2, 3)$ *belong to the same set* $S_{P(x)}(\alpha, \alpha + \delta)$ *for some* $0 \leq \alpha \leq 1$ *with* $0 \leq \delta \leq 1/4$. *Then, we have* $x_3 > \frac{1}{2}(P(x_1)/4)^{3/4}$.

Proof. For each $i = 1, 2, 3$, we have $P(x_i) \equiv 0 \pmod{p_1^f p_2^g}$, where $f = \lceil \alpha \log(P(x_1)/4)/\log p_1 \rceil$ and $g = \left\lceil \left(\frac{3}{4} - \alpha\right) \log(P(x_1)/4)/\log p_2 \right\rceil$.

We see that the congruent equation $X^2 + D \equiv 0 \pmod{p_1^f p_2^g}$ has exactly four distinct solutions $0 < X_1 < X_2 < X_3 < X_4 < p_1^f p_2^g$ with $X_1 + X_4 = X_2 + X_3 = p_1^f p_2^g$. Hence, we have $X_3, X_4 > \frac{1}{2} p_1^f p_2^g$ and $x_3 > \frac{1}{2} p_1^f p_2^g \geq \frac{1}{2}(P(x_1)/4)^{3/4}$. □

https://doi.org/10.1017/S0017089518000344 Published online by Cambridge University Press

3. Hypergeometric functions and finiteness results. Let $F(\alpha, \beta, \gamma, z)$ be the hypergeometric function given by the series

$$1 + \frac{\alpha \cdot \beta}{1 \cdot \gamma} z + \frac{\alpha(\alpha+1)\beta(\beta+1)}{1 \cdot 2 \cdot \gamma(\gamma+1)} z^2 + \cdots, \tag{2}$$

converging for all $|z| < 1$ and for $z = 1$ if $\gamma > \alpha + \beta$. Define $G(z) = G_{n_1,n_2}(z) = F(-\frac{1}{2} - n_2, -n_1, -n, z)$, $H(z) = H_{n_1,n_2}(z) = F(-\frac{1}{2} - n_1, -n_2, -n, z)$ and $E(z) = F(n_2 + 1, n_1 + \frac{1}{2}, n + 2, z)/F(n_2 + 1, n_1 + \frac{1}{2}, n + 2, 1)$ for positive integers n, n_1, n_2 with $n = n_1 + n_2$ and $n_1 \geq n_2$.

We quote some properties from Lemmas 2–4 of [**5**]:

(a) $\left|G(z) - \sqrt{1-z}H(z)\right| < z^{n+1}G(1)$,
(b) $\binom{n}{n_1}G(4z)$ and $\binom{n}{n_1}H(4z)$ are polynomials with integer coefficients of degree n_1 and n_2, respectively,
(c) $G(1) < G(z) < G(0) = 1$ for $0 < z < 1$,
(d) $G(1) = \binom{n}{n_1}^{-1} \prod_{m=1}^{n_1} \left(1 - \frac{1}{2m}\right)$ and
(e) $G_{n_1+1,n_2+1}(z)H_{n_1,n_2}(z) - G_{n_1,n_2}(z)H_{n_1+1,n_2+1}(z) = cz^{n+1}$ for some constant $c \neq 0$.

Now, we obtain the following upper bound for solutions of (1) relative to a given large one.

LEMMA 3.1. *Let α, δ and δ_1 be real numbers with $0 \leq \alpha < \alpha + \delta \leq 1$ and $0 < \delta_1 < 1/12$ and $A, B, w, q, s_1, k_1, l_1, s_2, k_2, l_2$ be nonnegative integers such that both $A^2 + D = w = 2^{s_1}p_1^{k_1}p_2^{l_1}$ and $B^2 + D = q = 2^{s_2}p_1^{k_2}p_2^{l_2}$ belong to $S(\alpha, \alpha + \delta; u, v)$ with $B > A$. Moreover, put $W_1 = (2^{772+210\delta}D^{241})^{1/(35(2-3\delta)-(3\delta+1)/2)}$, $W_2 = (2^{22/9+2\delta/3}3^{7/3})^{1/\delta_1}$ and $W = \max\{W_1, W_2\}$.*

If $w \geq W$, then $q < 4^{70}w^{71}$ or

$$q^{1-\frac{1}{2}\left(\frac{5}{3}+\delta+\delta_1\right)} < 2^{\frac{31}{9}+s_1+\frac{2}{3}\delta}3^{\frac{16}{3}}Dw^{\frac{19}{6}+\frac{3}{2}\delta-\frac{1}{2}\left(\frac{5}{3}+\delta+\delta_1\right)}. \tag{3}$$

Proof. Substituting $z = \frac{D}{w}$, we see that $\sqrt{1-z} = \frac{A}{w^{\frac{1}{2}}}$ and it follows from the property (b) that

$$\binom{n}{n_1}G(z) = \frac{P}{(4w)^{n_1}} \text{ and } \binom{n}{n_1}H(z) = \frac{Q}{(4w)^{n_2}} \tag{4}$$

for some integers P and Q.

Now, the property (a) gives

$$\left|\frac{P}{(4w)^{n_1}} - \frac{AQ}{w^{\frac{1}{2}}(4w)^{n_2}}\right| < \binom{n}{n_1}\left(\frac{D}{w}\right)^{n+1} G(1), \tag{5}$$

and therefore

$$\left|1 - \frac{AQ}{w^{\frac{1}{2}}(4w)^{n_2-n_1}P}\right| < \frac{(4w)^{n_1}}{|P|}\binom{n}{n_1}\left(\frac{D}{w}\right)^{n+1} G(1). \tag{6}$$

Letting

$$K = \left| \frac{B}{q^{\frac{1}{2}}} - \frac{AQ}{w^{\frac{1}{2}}(4w)^{n_2-n_1}P} \right|, \tag{7}$$

we have

$$K < \epsilon + \frac{(4w)^{n_1}}{|P|} \binom{n}{n_1} \left(\frac{D}{w}\right)^{n+1} G(1), \tag{8}$$

where

$$\epsilon = \left| \frac{B}{q^{\frac{1}{2}}} - 1 \right| < \frac{D}{2B^2}. \tag{9}$$

Let λ be the integer such that $(4w)^{\lambda-1} < (q/w)^{1/2} \le (4w)^{\lambda}$ and choose n_1, n_2 such that $\frac{2}{3}\lambda - \frac{2}{3} \le n_1 \le \frac{2}{3}\lambda + 1, n_2 = n_1 + \lambda$ and $K \ne 0$. Following the proof of Theorem 1 in [**5**], the property (e) allows such a choice. Moreover, we may assume without loss of generality that $q \ge 4^{70} w^{71}$, which yields that $\lambda \ge 35$ and $n_1 \ge 23$.

Let R be the l.c.m. of q and $w(4w)^{2\lambda}$. Then, since $k_1 \equiv l_1, k_2 \equiv l_2 \pmod 2$ and we have chosen n_1, n_2 such that $K \ne 0$, we see that the denominator of K must divide $R^{1/2}|P|$.

Since both w and q belong to $S(\alpha, \alpha+\delta; u, v)$, we have $p_1^{k_2} \le (q/2^{s_2})^{\alpha+\delta} \le (2^{4\lambda-s_2} w^{2\lambda+1})^{\alpha+\delta}$ and $p_2^{l_2} \le (q/2^{s_2})^{1-\alpha} \le (2^{4\lambda-s_2} w^{2\lambda+1})^{1-\alpha}$, $p_1^{k_1} \le w^{\alpha+\delta}$ and $p_2^{l_1} \le w^{1-\alpha}$. Hence, we see that $R \le 2^{8\lambda+(2\lambda+1)s_1+(4\lambda-s_2)\delta} w^{(1+\delta)(2\lambda+1)}$ and

$$K \ge \frac{1}{|P|\sqrt{R}} \ge \frac{1}{|P|\, w^{(1+\delta)\left(\lambda+\frac{1}{2}\right)} 2^{(4+2\delta+s_1)\lambda + \frac{s_1-s_2\delta}{2}}}. \tag{10}$$

Combining (8) and (10), we have

$$\begin{aligned} &\epsilon\, |P|\, w^{(1+\delta)\left(\lambda+\frac{1}{2}\right)} 2^{(4+2\delta+s_1)\lambda+\frac{s_1-s_2\delta}{2}} \\ &\quad > 1 - 2^{2n_1+(4+2\delta+s_1)\lambda+\frac{s_1-s_2\delta}{2}} w^{n_1+(1+\delta)\left(\lambda+\frac{1}{2}\right)} \binom{n}{n_1} \left(\frac{D}{w}\right)^{n+1} G(1). \end{aligned} \tag{11}$$

Since $G(1)\binom{n}{n_1} = \prod_{1\le m\le n_1}\left(1 - \frac{1}{2m}\right) < \frac{1}{8}$ for $n_1 \ge 23$, the last term of (11) is at most

$$\begin{aligned} &2^{2n_1+(4+2\delta+s_1)\lambda+\frac{s_1-s_2\delta}{2}} w^{n_1+(1+\delta)\left(\lambda+\frac{1}{2}\right)} \left(\frac{D}{w}\right)^{n+1} \\ &\quad \le 2^{2n_1+(4+2\delta+s_1)\lambda+\frac{s_1-s_2\delta}{2}} w^{n_2+\delta\lambda+\frac{1+\delta}{2}-(n+1)} D^{n+1} \\ &\quad = 2^{(4+2\delta+s_1)\lambda+\frac{s_1-s_2\delta}{2}} w^{\delta\lambda+\frac{\delta-1}{2}} D^{\lambda} \left(\frac{4D^2}{w}\right)^{n_1} \\ &\quad \le 2^{\left(\frac{16}{3}+2\delta+s_1\right)\lambda-\frac{1}{3}} w^{\left(\delta-\frac{2}{3}\lambda\right)+\frac{\delta}{2}+\frac{1}{6}} D^{\frac{7}{3}\lambda-\frac{4}{3}} \\ &\quad = \frac{w^{\frac{1}{6}+\frac{\delta}{2}}}{2^{\frac{1}{3}} D^{\frac{4}{3}}} \left(\frac{2^{16+6\delta+3s_1} D^7}{w^{2-3\delta}}\right)^{\frac{\lambda}{3}} \\ &\quad \le \frac{1}{2}, \end{aligned} \tag{12}$$

https://doi.org/10.1017/S0017089518000344 Published online by Cambridge University Press

provided that $w^{35(2-3\delta)-(3\delta+1)/2} \geq 2^{562+210\delta+105s_1} D^{241}$, which follows from our assumption that $w \geq W \geq W_1$. Hence, we have

$$\epsilon \, |P| \, w^{(1+\delta)(\lambda+\frac{1}{2})} 2^{(4+s_1)\lambda+\frac{s_1-s_2}{2}} > \frac{1}{2}. \tag{13}$$

By the property (c), we have, with the aid of Lemma 5 of **[5]**,

$$\begin{aligned} |P| &< (4w)^{n_1} \binom{n}{n_1} \\ &< \frac{1}{2} \left(\frac{3}{4^{1/3}} \right)^{\frac{7}{3}\lambda+2} (4w)^{\frac{2}{3}\lambda+1} \\ &= 2^{-\frac{2}{9}\lambda-\frac{1}{3}} 3^{\frac{7}{3}\lambda+2} w^{\frac{2}{3}\lambda+1}. \end{aligned} \tag{14}$$

Now, by our assumption that $w \geq W \geq W_2$, we have

$$2^{\frac{4}{9}+\frac{2}{3}\delta+s_1} 3^{\frac{7}{3}} < (4w)^{\delta_1}, \tag{15}$$

and therefore

$$\begin{aligned} |P| \, w^{(1+\delta)(\lambda+\frac{1}{2})} 2^{(4+2\delta+s_1)\lambda+1} &< 2^{\left(\frac{34}{9}+2\delta+s_1\right)\lambda+\frac{2}{3}} 3^{\frac{7}{3}\lambda+2} w^{\left(\frac{5}{3}+\delta\right)\lambda+\frac{3+\delta}{2}} \\ &= 2^{\frac{2}{3}} 3^2 w^{\frac{3+\delta}{2}} (2^{\frac{4}{9}+s_1-\frac{4}{3}\delta} 3^{\frac{7}{3}})^{\lambda} (4w)^{\left(\frac{5}{3}+\delta\right)\lambda} \\ &\leq 2^{4+2\delta} 3^2 w^{\frac{19}{6}+\frac{3}{2}\delta} (2^{\frac{4}{9}+s_1-\frac{4}{3}\delta} 3^{\frac{7}{3}})^{\lambda} \left(\frac{q}{w} \right)^{\frac{1}{2}\left(\frac{5}{3}+\delta\right)} \\ &\leq 2^{\frac{40}{9}+s_1+\frac{2}{3}\delta} 3^{\frac{13}{3}} w^{\frac{19}{6}+\frac{3}{2}\delta} \left(\frac{q}{w} \right)^{\frac{1}{2}\left(\frac{5}{3}+\delta+\delta_1\right)}. \end{aligned} \tag{16}$$

Combining (13) and (16), we have

$$2^{\frac{40}{9}+s_1+\frac{2}{3}\delta} 3^{\frac{13}{3}} w^{\frac{19}{6}+\frac{3}{2}\delta} \left(\frac{q}{w} \right)^{\frac{1}{2}\left(\frac{5}{3}+\delta+\delta_1\right)} > \frac{1}{2\epsilon} > \frac{2q}{3D} \tag{17}$$

and (3) immediately follows. □

4. Arithmetic of quadratic fields and the stronger gap principle. In this section, we shall prove a gap principle for larger solutions using some arithmetic of quadratic fields.

Let d be the unique squarefree integer such that $D = B^2 d$ for some integer B. If $p_i (i = 1, 2)$ splits (or is ramified) in $\mathbb{Q}(\sqrt{-d})$, then we can factor $[p_i] = \mathfrak{p}_i \bar{\mathfrak{p}}_i$ using some prime ideal $\mathfrak{p}_i$ in $\mathbb{Q}(\sqrt{-d})$ (we note that if p_i is ramified in $\mathbb{Q}(\sqrt{-d})$, then $\mathfrak{p}_i = \bar{\mathfrak{p}}_i$). Moreover, if $[\alpha] = [\beta]$ in $\mathbb{Q}(\sqrt{-d})$, then $\alpha = \theta\beta$, where θ is a sixth root of unity if $d = 3$, a fourth root of unity if $d = 1$ and ± 1 otherwise.

Assume that $A^2 + D = A^2 + B^2 d = 2^{2e} p_1^k p_2^l$ with $e \in \{0, 1\}$. If both of p_i's are splitting or ramified, then, we must have $[(A + B\sqrt{-d})/(2^e p_1^{k^*} p_2^{l^*})] = \mathfrak{p}_1^{k'} \mathfrak{p}_2^{l'}, \bar{\mathfrak{p}}_1^{k'} \mathfrak{p}_2^{l'}, \mathfrak{p}_1^{k'} \bar{\mathfrak{p}}_2^{l'}$ or $\bar{\mathfrak{p}}_1^{k'} \bar{\mathfrak{p}}_2^{l'}$, where k^*, l^*, k', l' are some nonnegative integers with $k = 2k^* + k'$ and $l = 2l^* + l'$. If p_1, say, is inert in $\mathbb{Q}(\sqrt{-d})$, then k is even and $[p_1]$ divides both $[(A + B\sqrt{-d})/2^e]$ and $[(A - B\sqrt{-d})/2^e]$ exactly $k/2$ times. Hence, in any case, we have

$$\left[\frac{A+B\sqrt{-d}}{A-B\sqrt{-d}}\right]=\left(\frac{\bar{\mathfrak{p}}_1}{\mathfrak{p}_1}\right)^{\pm k'}\left(\frac{\bar{\mathfrak{p}}_2}{\mathfrak{p}_2}\right)^{\pm l'} \tag{18}$$

with $0 \le k' \le k$ and $0 \le l' \le l$ for some appropriate choices of signs.

We shall show a gap principle for solutions much stronger than Lemmas 2.1 and 2.2.

LEMMA 4.1. *Let c denote the constant $\sqrt{\log 2 \log 3/2^{7/2}} = 0.2594\ldots$ If $x_3 > x_2 > x_1 > 10^6 D$ belong to the same set $S^{(j)}$ with $j = 0$ or 3 and $y_i = x_i^2 + D$ for $i = 1, 2, 3$, then $y_3 > \exp(c y_1^{1/8})$. Furthermore, if $x_4 > x_3 > x_2 > x_1 > 10^6 D$ belong to the same set $S^{(j)}$ with $j = 1$ or 2 and $y_i = x_i^2 + D$ for $1 \le i \le 4$, then $y_4 > \exp(c y_1^{1/8})$.*

Proof. Assume that $S^{(j)}$ has three elements $x_1 < x_2 < x_3$ in the case $j = 0, 3$ and four elements $x_1 < x_2 < x_3 < x_4$ in the case $j = 1, 2$. By Lemmas 2.1 and 2.2, we have $x_3 > x_2 > \frac{1}{2}(y_1/4)^{3/4} > \frac{1}{2^{5/2}} x_1^{3/2}$ and we have $x_4 > x_3 > \frac{1}{2}(y_1/4)^{3/4} > \frac{1}{2^{5/2}} x_1^{3/2}$ in both cases, respectively. So that, setting $(X_1, X_2, X_3) = (x_1, x_2, x_3)$ in the case $j = 0, 3$ and $(X_1, X_2, X_3) = (x_1, x_3, x_4)$ in the case $j = 1, 2$, we have $X_3 > X_2 > \frac{1}{2^{5/2}} X_1^{3/2}$ in any case.

Let $X_i^2 + D = 2^{s_i} p_1^{k_i} p_2^{l_i}$ for each $i = 1, 2, 3$ and $K = \max k_i$, $L = \max l_i$. Then, (18) yields that

$$\left[\frac{X_i+\sqrt{-D}}{X_i-\sqrt{-D}}\right]=\left(\frac{\bar{\mathfrak{p}}_1}{\mathfrak{p}_1}\right)^{\pm k_i'}\left(\frac{\bar{\mathfrak{p}}_2}{\mathfrak{p}_2}\right)^{\pm l_i'} \tag{19}$$

with $0 \le k_i' \le k_i$ and $0 \le l_i' \le l_i$, for each $i = 1, 2, 3$. Now, we can take some integers e_1, e_2, e_3 which are not all zero so that

$$\left[\frac{X_1+\sqrt{-D}}{X_1-\sqrt{-D}}\right]^{e_1}\left[\frac{X_2+\sqrt{-D}}{X_2-\sqrt{-D}}\right]^{e_2}\left[\frac{X_3+\sqrt{-D}}{X_3-\sqrt{-D}}\right]^{e_3}=[1]. \tag{20}$$

Indeed, if (k_1', k_2', k_3') and (l_1', l_2', l_3') are not proportional, then we can take $e_1 = \pm k_2' l_3' \pm k_3' l_2'$, $e_2 = \pm k_3' l_1' \pm k_1' l_3'$, $e_3 = \pm k_1' l_2' \pm k_2' l_1'$ with appropriate signs. In the case (k_1', k_2', k_3') and (l_1', l_2', l_3') are proportional, we can take $(e_{i_1}, e_{i_2}, e_{i_3}) = (k_{i_2}', -k_{i_1}', 0)$ or $(l_{i_2}', -l_{i_1}', 0)$ for some permutation (i_1, i_2, i_3) of $(1, 2, 3)$ so that e_i's are not all zero. In other words, we have

$$\left(\frac{X_1+\sqrt{-D}}{X_1-\sqrt{-D}}\right)^{fe_1}\left(\frac{X_2+\sqrt{-D}}{X_2-\sqrt{-D}}\right)^{fe_2}\left(\frac{X_3+\sqrt{-D}}{X_3-\sqrt{-D}}\right)^{fe_3}=1, \tag{21}$$

where $f = 6$ if $d = 3$, 4 if $d = 1$ and 2 otherwise. This implies that

$$\Lambda = e_1 \arg(X_1+\sqrt{-D}) + e_2 \arg(X_2+\sqrt{-D}) + e_3 \arg(X_3+\sqrt{-D}) \tag{22}$$

must be a multiple of $2\pi/f$.

If $\Lambda \ne 0$, then we see that $\left(\frac{|e_1|}{X_1}+\frac{|e_2|}{X_2}+\frac{|e_3|}{X_3}\right)\sqrt{D} > |\Lambda| \ge 2\pi/f$, and therefore $2.01 f KL\sqrt{D} \ge 2X_1\pi$ and $1.92KL\sqrt{D} > X_1$. Since $X_1 = x_1 > 10^6 D$, we have $1.92KL > 2\sqrt{X_1} > (X_1^2 + D)^{1/4} = y^{1/4}$.

Assume that $\Lambda = 0$. If $e_1 = 0$, then we must have $\Lambda = e_2 \arg(X_2 \pm \sqrt{-D}) + e_3 \arg(X_3 \pm \sqrt{-D}) = 0$ and $(X_2^2 + D)^{e_2} = (X_3^2 + D)^{e_3}$. Hence, we must

https://doi.org/10.1017/S0017089518000344 Published online by Cambridge University Press

have $|e_2| > |e_3| > 0$ and $\left|\arg(X_2 \pm \sqrt{-D})\right| > \left|\arg(X_3 \pm \sqrt{-D})\right| > 0$ from $X_3 > X_2$ and $\Lambda \neq 0$, which is a contradiction. Thus, e_1 cannot be zero. The triangle inequality immediately gives that $\left|\arg(X_1 \pm \sqrt{-D})\right| \leq \left|e_2 \arg(X_2 \pm \sqrt{-D})\right| + \left|e_3 \arg(X_3 \pm \sqrt{-D})\right|$, and therefore

$$\frac{1}{\sqrt{X_1^2 + D}} < \frac{e_2}{X_2} + \frac{e_3}{X_3} < \frac{2KL}{X_2} < \frac{8\sqrt{2}KL}{(X_1^2 + D)^{\frac{3}{4}}}. \tag{23}$$

Thus, we obtain $8\sqrt{2}KL > (X_1^2 + D)^{1/4} = y_1^{1/4}$.

Hence, in any case we have $8\sqrt{2}KL > y_1^{1/4}$ and $\max\{K \log p_1, L \log p_2\} > y_1^{1/8}\sqrt{\log p_1 \log p_2/(8\sqrt{2})}$. Thus, we conclude that

$$X_3^2 + D \geq \max\{p_1^K, p_2^L\} > \exp\left(y_1^{\frac{1}{8}}\sqrt{\frac{\log p_1 \log p_2}{8\sqrt{2}}}\right) \geq \exp\left(cy_1^{\frac{1}{8}}\right), \tag{24}$$

proving the Lemma. □

5. Proof of the theorem. We set $\delta_1 = 0.04377667$. We shall begin by proving (i).

Let $y_1 = x_1^2 + D$ be the smallest solution in a given class $S^{(j)}(W, \infty; u, v)$ and $y_2 = x_2^2 + D$ be the third or fourth smallest one in this class for $j = 0, 3$ or $j = 1, 2$, respectively. Lemma 3.1 with $\delta = 1/4$ gives that

$$y_2 < \max\left\{4^{70}y_1^{71}, (2^{\frac{101}{18}}3^{\frac{16}{3}}Dy_1^{\frac{31}{12}-\frac{\delta_1}{2}})^{1/\left(\frac{1}{24}-\frac{\delta_1}{2}\right)}\right\}. \tag{25}$$

But Lemma 4.1 immediately yields that $y_2 > \exp(cy_1^{1/8})$. We observe that these two inequalities are incompatible for $y_1 \geq W = \max\{W_1, W_2\}$. Hence, we see that $\#S^{(j)}(W, \infty; u, v) \leq 2$ for each j, u, v for $j = 0, 3$ and $\#S^{(j)}(W, \infty; u, v) \leq 3$ for each j, u, v for $j = 1, 2$. Combining these estimates, we obtain $\#S(0, 1, W, \infty) \leq 30$ after the easy observation that $S(0, 1, W, \infty; 0, 0)$ must be empty since $W > D^2$. This proves (i).

Now, we shift our concern to smaller solutions. Let $f(y) = y^{3/2}/2^{5/2}$, $g(y) = \exp(cy_1^{1/8})$ and $f^{(m)}$ be the mth iteration of f. $y_1 = x^2 + D = 2^s p_1^k p_2^l$ denotes the smallest solution. We have the following three cases.

Case 1. $D \geq Y$ or $y_1 \geq Y$.

If $D \geq Y$, then $W = W_1 < g(f^{(3)}(D)) \leq g(f^{(3)}(y_1))$. If $D \leq Y - 1$ and $y_1 \geq Y$, then we have that $W = W_2 < g(f^{(3)}(Y)) \leq g(f^{(3)}(y_1))$. Hence, we always have $W \leq g(f^{(3)}(y_1))$ in Case 1, and therefore, using Lemmas 2.1 and 2.2, we obtain $\#S^{(j)}(y_1, W) \leq 9$ if $j = 0, 3$ and $\#S^{(j)}(y_1, W) \leq 5$ if $j = 1, 2$. So that, $\#S(0, 1, 0, \infty) \leq 30 + 28 = 58$. This proves (ii).

Case 2. $D, y_1, p_2 \leq Y - 1$.

Let $W_3 = f^{(2)}(Y) = 3545401233665.83\ldots$ Since $y_1 \leq Y - 1$, then $D \leq y_1 \leq Y - 1$ and $p_1 \leq y_1 \leq Y - 1$. A computer search revealed that $\#S(0, 1, 0, W_3) \leq 13$ for any $D, p_1, p_2 \leq Y - 1$. Since $W < g(f^{(3)}(Y)) = g(f(W_3))$, from Lemmas 2.1 and 2.2, we see that $\#S^{(j)}(W_3, W) \leq 5$ if $j = 0, 3$ and $\#S^{(j)}(W_3, W) \leq 3$ if $j = 1, 2$. This proves (iii).

https://doi.org/10.1017/S0017089518000344 Published online by Cambridge University Press

Case 3. $D, y_1 \leq Y-1$ and $p_2 \geq Y$.

If $x^2 + D = 2^s p_1^k p_2^l \leq Y - 1$, then, since $p_2 \geq Y$, we must have $x^2 + D = 2^s p_1^k$, which has at most five solutions from the results mentioned in the introduction. The number of the other solutions can be bounded as in Case 2 and we obtain (iv). This completes the proof of the Theorem.

REFERENCES

1. R. Apéry, Sur une équation diophantinne, *C. R. Acad. Sci. Paris, Sér. A* **251** (1960), 1451–1452.

2. E. A. Bender and N. P. Herzberg, *Some diophantine equations related to the quadratic form* $ax^2 + by^2$, *Studies in Algebra and Number Theory* (Academic Press, New York, 1979), 219–272.

3. M. A. Bennett and C. M. Skinner, Ternary diophantine equations via Galois representations and modular forms, *Can. J. Math.* **56** (2004), 23–54.

4. A. Bérczes and I. Pink, On generalized Lebesgue-Ramanujan–Nagell equations, *An. Şt. Univ. Ovivius Constanţa* **22** (2014), 51–71.

5. F. Beukers, On the generalize Ramanujan–Nagell equation I, *Acta Arith.* **38** (1980/81), 389–410.

6. F. Beukers, On the generalize Ramanujan–Nagell equation II, *Acta Arith.* **39** (1981), 123–132.

7. Y. Bilu, G. Hanrot and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.* **539** (2001), 75–122.

8. Y. Bugeaud, On some exponential diophantine equations, *Monatsh. Math.* **132** (2001), 93–97.

9. Y. Bugeaud, M. Mignotte and S. Siksek, Classical and modular approaches eto exponential diophantine equations II. The Lebesgue–Nagell equation, *Compos. Math.* **142** (2006), 31–62.

10. Y. Bugeaud and T. N. Shorey, On the number of solutions of the generalized Ramanujan–Nagell equation, *J. Reine Angew. Math.* **539** (2001), 55–74.

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

12. J.-H. Evertse, On equations in S-units and the Thue–Mahler equation, *Inv. Math.* **75** (1984), 561–584.

13. H. Godinho, D. Marques and A. Togbé, On the diophantine equation $x^2 + C = y^n$ for $C = 2^a 3^b 17^c$ and $C = 2^a 13^b 17^c$, *Math. Slovaca* **66** (2016), 565–574.

14. Y. Hu and M. Le, On the number of the generalized Ramanujan–Nagell equation $D_1 x + D_2^m = p^n$, *Bull. Math. Soc. Sci. Math. Roumanie* **55** (2012), 279–293.

15. M. Le, The divisibility of the class number for a class of imaginary quadratic fields, *Kexue Tongbao* **32** (1987), 724–727 (in Chinese).

16. M. Le, The diophantine equation $x^2 + D^m = p^n$, *Acta Arith.* **52** (1989), 225–235.

17. M. Le, Diophantine equation $x^2 + 2^m = y^n$, *Chinese Sci. Bull.* **42** (1997), 1515–1517.

18. M. Le, On the diophantine equation $x^2 + D = 4p^n$, *J. Number Theory* **41** (1997), 87–97.

19. M. Le, On the diophantine equation $D_1 x^2 + D_2 = 2^{n+2}$, *Acta Arith.* **64** (1993), 29–41.

20. M. Le, A note on the number of solutions of the generalized Ramanujan–Nagell equation $D_1 x^2 + D_2 = 4p^n$, *J. Number Theory* **62** (1997), 100–106.

21. M. Le, On the diophantine equation $(x^3-1)/(x-1) = (y^n-1)/(y-1)$, *Trans. Amer. Math. Soc.* **351** (1999), 1063–1074.

22. M. Lebesgue, Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$, *Nouv. Ann. Math.* **9** (1850), 178–180.

23. M.-G. Leu and G.-W. Li, The diophantine equation $2x^2 + 1 = 3^n$, *Proc. Amer. Math. Soc.* **131** (2003), 3643–3645.

24. W. Ljunggren, Noen setninger om ubestemte likninger av formen $\frac{x^n-1}{x-1} = y^q$, *Norsk. Mat. Tidsskr.* **25** (1943), 17–20.

25. T. Nagell, Sur l'impossibilité de quelques équations a deux indetérminées, *Norsk Mat. Foreninngs Skrifter I* Nr. **13** (1923), 1–18.

26. T. Nagell, The diophantine equation $x^2 + 7 = 2^n$, *Nork. Mat. Tidsskr.* **30** (1948), 62–64 (in Norwegian), English version: *Ark. Mat.* **4** (1960), 185–187.

27. I. Pink, On the diophantine equation $x^2 + 2^\alpha 3^\beta 5^\gamma 7^\delta = y^n$, *Publ. Math. Debecen* **70** (2007), 149–166.

28. T. N. Shorey, A. J. van der Poorten, R. Tijdeman and A. Schinzel, Applications of the Gel'fond–Baker method to diophantine equations, in *Transcendence theory: Advances and applications* (Academic Press, London, 1977), 59–77.

29. C. Skinner, The diophantine equation $x^2 = 4q^n - 4q + 1$, *Pacific J. Math.* **139** (1989), 303–309.

30. T. Skolem, The use of p-adic method in the theory of diophantine equations, *Bull. Soc. Math. Belg.* **7** (1955), 83–95.

31. R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. Math.* **141** (1995), 553–572.

32. A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. Math.* **141** (1995), 443–551.

33. P. Yuan and Y. Hu, On the diophantine equation $x^2 + D^m = p^n$, *J. Number Theory* **111** (2005), 144–153.